P660HW-B1A Telefonica
User Manual

V1.00

Contents

1 Introduction 1
1.1 Application 1
1.2 Features 2
1.3 Wireless Specifications 3
1.4 Compliance Certificates 4
1.5 Standards Compatibility and Compliance 4
1.6 Supported Encapsulation 5
1.7 Environment Requirements 5
1.8 System Requirements 5
1.9 Safety Precautions 9
1.10 LED Status Description 10
1.10.1 Front Panel 10
1.10.2 Rear Panel 12
2 Hardware Installation 12
2.1 Choosing the Best Location for Wireless Operation 13
2.2 Connecting the ADSL Router 14
2.3 Factory Reset Button 14
3 Introduction to Web Configuration 15
3.1 Preparation before Login 15
3.2 Logging In to the Router 16
3.2.1 First-Time Login 16
3.3 Device Info 17
3.3.1 Summary of Device Information 18
3.3.2 WAN Interface Information 18
3.3.3 Statistics 19
3.3.4 Route Table Information 22
3.3.5 ARP Table Information 22
3.3.6 DHCP 22
3.4 Advanced Setup 23
3.4.1 WAN Configuration 23
3.4.2 LAN Configuration 40
3.4.3 NAT 41
3.4.4 Security 50
3.4.5 Quality of Service 52
3.4.6 Routing 62

3.4.7 DNS 64
3.4.8 DSL 66
3.4.9 Port Mapping 67
3.4.10 IPSec 68
3.4.11 Certificate 69
3.5 Wireless 72
3.5.1 Wireless LAN Basics 73
3.5.2 Wireless – Basic 76
3.5.3 Wireless – Security 77
3.5.4 Wireless - MAC Filter 87
3.5.5 Wireless – Bridge 88
3.5.6 Wireless – Advanced 90
3.5.7 Wireless – Station Info 93
3.6 Diagnostics 93
3.7 Management 94
3.7.1 Settings 94
3.7.2 System Log 95
3.7.3 TR-069 Client 97
3.7.4 Internet Time 98
3.7.5 Access Control 99
3.7.6 Update Software 100
3.7.7 Save/Reboot 101

1 Introduction

The P660HW-B1A Telefonica is a highly ADSL2+ Integrated access device and can support ADSL link with downstream up to 24 Mbps and upstream up to 1 Mbps. It is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or 802.11b/g wireless network. The Router combines high-speed ADSL Internet connection, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.

The P660HW-B1A Telefonica is easy to install and use. The router connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet by a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

Network and Router management is done through the web-based management interface that can be accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

The embedded 802.11g wireless access point provides Internet access and connectivity to the Ethernet for 802.11g and 802.11b wireless workstations. IEEE 802.11g is fully compatible with IEEE 802.11b wireless devices. The 802.11g standard supports data transfer with rate up to 54 Mbps. The wireless access point (AP) of the router supports common security protocols that are used for wireless LAN, including 64/128 bits WEP encryption, 802.1x, WPA and WPA2.

1.1 Application

- Home gateway
- SOHOs
- Small enterprises
- TV over IP (IPTV)
- Higher data rate broadband sharing

- Broadband Internet access sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

1.2 Features

- ADSL2+ interface complied with G.dmt, G.lite, T1.413, G.992.3 (ADSL/ADSL2), G.992.5(ADSL2+), Annex A, Annex L.
- Hardware ATM segmentation & reassembly engine with CBR, rt- VBR, nrt-VBR, UBR- with-PCR, UBR
- 4 x 10/100BASE-T/TX Ethernet switch ports
- IEEE802.11 b/g compatible wireless AP
- Support 64/128-bit WEP, 802.1x, WPA, and WPA2 for wireless security
- Firmware upgrade: Telnet, HTTP Web Management, TFTP, FTP
- VPN Pass Through on L2TP, PPTP, IPSec
- Transparent Bridging among 10/100 Mbps Ethernet, and 802.11g wireless LAN
- Backup and restoration of the configuration file
- Support DHCP server/client/relay
- Support self-learning bridge (IEEE 802.1D Transparent Bridging)
- Support 64 learning MAC addresses at least
- Support IP source and destination routing
- Support address filtering, UPnP, NAT, NAPT, DMZ, IP QoS
- Supporting up to 8 PVCs
- Support ATM forum UNI3.0, 3.1 and 4.0 Permanent Virtual Circuits (PVCs)
- Support ITU-T i.610F4/F5 Operation, Administration, and Maintenance (OAM)
- Command line interface via serial port, telnet, or ssh
- Date and time update from Simple Network Time Server (SNTP)
- Three-level usernames and passwords: admin, user, and support
- Service access control based on incoming interface: WAN or LAN
- Protect Denial of Service (DoS) attacks from WAN/LAN: SYN flooding, IP surfing, ping of Death, fraggle,- UDP ECHO (port 7) , teardrop, land
- PAP (RFC1334), CHAP (RFC1994), MSCHAP for PPP session
- Support auto channeling for wireless

- Support a main SSID and a guest SSID for wireless
- Support RTS/CTS, segment function for wireless
- Support STA mutual isolation for wireless
- Support SES for wireless
- support WDS for wireless
- Support Hide SSID for wireless
- Support MAC access/deny list for wireless
- WMM support for wireless
- PRE 54M: -66 dBm@10%PER; 11M: -80 dBm@8%PER for wireless
- Industry standard and interoperable DSL interface

1.3 Wireless Specifications

Item	Description	
Network Standard	● IEEE 802.11b ● IEEE 802.11g	
Frequency Range	2.40 GHz~2.4835 GHz ISM band	
Modulation	● 802.11b: DBPSK, DQPS, CCK ● 802.11g: BPSK, QPSK, 16QAM, 64QAM	
RF Power	20 dBm (Max). Typ. 18 dBm @Normal Temp Range, 802.11g: Typ. 15 dBm @ Normal Temp Range	
AP Capacity	Access User Quantity	50 Pcs~80 Pcs/AP (Proposal)
	Channel	● 11 (US and Canada) ● 13 (Europe and China) ● 14 (Japan)
	Auto-sensing Data Rate	● 802.11.b: 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps ● 802.11g: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps
Payload Rate	1 Mbps	DBPSK @ 0.81 Mbps
	2 Mbps	DQPSK @ 1.58 Mbps
	5.5 Mbps	CCK @ 4.07 Mbps
	6 Mbps	BPSK @ 4.64 Mbps

Item	Description	
	9 Mbps	BPSK @ 6.55 Mbps
	11 Mbps	CCK @ 7.18 Mbps
	12 Mbps	BPSK @ 8.31 Mbps
	18 Mbps	QPSK @ 11.5 Mbps
	24 Mbps	6QAM @ 14.18 Mbps
	36 Mbps	16QAM @ 18.31 Mbps
	48 Mbps	64QAM @ 23.25 Mbps
	54 Mbps	64QAM @ 26.12 Mbps
Security	64-bit/128-bit WEP, 802.1x, WPA, WPA2	
User Isolation	MAC Level	
MAC Filter	● Interface MAC Filter: Support ● Vacancy MAC Filter: Support	
Authentication	● DHCP Client & Static IP: Support ● 802.1X and Radius Client: Support ● DHCP Server: Support	
Radio Cover Range	● Outdoor: 120m~400m ● Indoor: 35m~100m	
Antenna Type	Internal Diversity with Connector. 3 dBi	

1.4 Compliance Certificates

- FCC Class B
- CE Mark

1.5 Standards Compatibility and Compliance

- RFC 2684 multi-protocol Encapsulation over ATM Adaptation Layer 5
- RFC1483 Multi-protocol Encapsulation over ATM Adaptation Layer 5
- RFC2364 PPP over ATM ALL5 (PPPoA)
- RFC2516 PPP Over Ethernet (PPPoE)
- RFC1662 PPP in HDLC-like Framing
- RFC1332 PPP Internet Protocol Control Protocol
- RFC1577/2225 Classical IP and ARP over ATM (IPoA)

- RFC1483R
- RFC894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC1042 A standard for the Transmission of IP Datagrams over IEEE 802 Networks
- MER (IP over Ethernet over AAL5)
- Support Application Level Gateways (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ANSI T1.413 issue 2
- IEEE802.3
- IEEE802.3u
- IEEE 802.11b
- IEEE 802.11g

1.6 Supported Encapsulation

- RFC 1483 bridge
- RFC 1483 Router
- Classical IP over ATM (RFC 1577)
- PPP over ATM (RFC 2364)
- PPP over Ethernet (RFC 2516)

1.7 Environment Requirements

- Operating temperature: 0ºC~40ºC (32ºF to 104ºF)
- Storage temperature: -20ºC~70ºC (-4ºF to 158ºF)
- Operating humidity: 10%~95%, non-condensing
- Storage humidity: 5%~95%, non-condensing

1.8 System Requirements

Recommended system requirements are as follows:

- Pentium 233 MHZ or above

- Memory: 64 Mbps or above
- 10M Base-T Ethernet or above
- Windows 9x, Windows 2000, Windows XP, Windows ME, Windows NT
- Ethernet network interface card (NIC)

The following information is very helpful for your ADSL configuration. To keep a record for reference, fill in the column as follows.

Collect the following information from your ADSL service provider.

Item	Description	Enter Information in This Column
VPI	Most users are not required to change this setting. The virtual path identifier (VPI) is used in conjunction with the virtual channel identifier (VCI) to identify the data path between the network of your ADSL service provider and your computer. If you set up the Router for multiple virtual connections, you need to configure the VPI and VCI as instructed by your ADSL service provider for additional connections. You can change this setting by accessing the WAN menu of the web management interface.	
VCI	Most users are not required to change this setting. The VCI used in conjunction with the VPI to identify the data path between the network of your ADSL service provider and your computer. If you set up the Router for multiple virtual connections, you need to configure the VPI and VCI as instructed by your ADSL service provider for additional connections. You can change this setting by accessing the WAN menu of the web management interface.	

Item	Description	Enter Information in This Column
Connection and Encapsulation Type	This is the method your ADSL service provider uses to transmit data between the Internet and your computer. Most users use the default PPPoE/PPPoA connection type. The Setup Wizard can be used to configure a PPPoE/PPPoA connection type. You may need to specify one of the following connection types: PPPoE LLC, PPPoA LLC and PPPoA VC-MUX. Other available connections and encapsulation combinations must be configured by using the Web manager. These include the Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC-MUX), Static IP (Bridged IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP LLC, 1483 Routed IP VC-MUX or IPoA), etc.	
Username	This is the user name used to log in to the network of your ADSL service provider. It is usually in the form of user@isp.com. Your ADSL service provider uses this to identify your account.	
Password	This is the password used, in conjunction with the user name previously mentioned, to log in to the network of your ADSL service provider. It is used to verify the identity of your account.	

Necessary information about your Router Residential Gateway is as follows.

Item	Description	Enter Information in This Column
LAN IP addresses for the Router	This is the IP address you enter in the **Address** field in the Web browser to access the configuration graphical user interface (GUI) of the gateway. The default IP address is **192.168.1.1** and it is referred to as the "Management IP" address in this User Manual. You can change this to suit any desired IP address scheme. This address is the basic IP address used for DHCP service on the LAN when DHCP is enabled.	
LAN Subnet Mask for the Router	This is the subnet mask used by the Router, and is used throughout your LAN. The default subnet mask is **255.255.255.0**. You can change it later.	
Username	This is the user name used to access the management interface of the gateway, when you attempt to connect to the device through a web browser. The default username of the Router is **admin**. It cannot be changed.	
Password	This is the password required when you access the management interface of the gateway. The default password is **admin**. It cannot be changed.	

Necessary information about your LAN or computer is as follows.

Item	Description	Enter Information in This Column
Ethernet NIC	If your computer has an Ethernet NIC, you can connect the Router to this Ethernet port using an Ethernet cable. You can also use the	

Item	Description	Enter Information in This Column
	Ethernet ports on the Router to connect to other computer or Ethernet devices.	
DHCP Client status	By default, your Router Residential Gateway is configured as a DHCP server. This means that it can assign an IP address, a subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses that the Router assigns is from **192.168.1.2** to **192.168.1.254**. You need to set your computer (or computers) to **Obtain an IP address automatically** (that is, to set computers as DHCP clients.)	

1.9 Safety Precautions

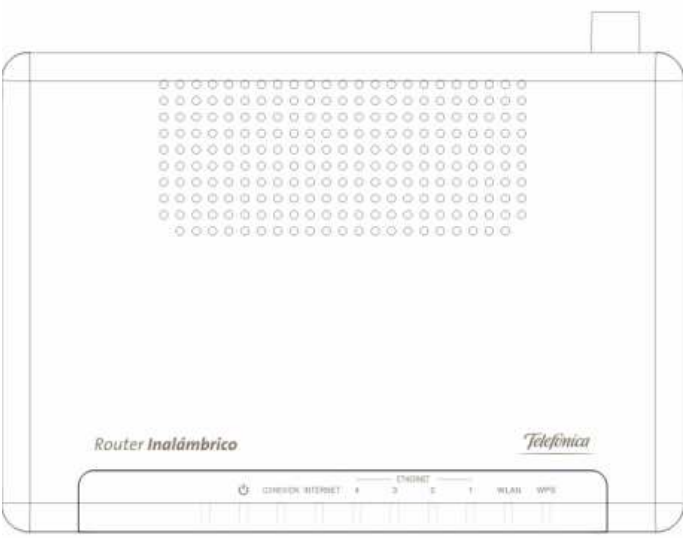
Follow the announcements below to protect the device from risks and damage caused by fire and electric power.

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat radiation is necessary to avoid any damage caused by overheating to the device. The holes are designed for heat radiation to ensure that the device works normally. Do not cover these heat radiant holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.

- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.
- Do not place this device on an unstable surface or support.

1.10 LED Status Description

1.10.1 Front Panel



The following table describes the LED status of the Router:

LED	Status	Description
Power	Off	Router not powered-on.
	Green	The power is on and the device operates normally.
	Red	The power is self-testing.
		The device enters the console mode of the boot loader.

LED	Status	Description
		The self-testing of the power fails if the LED is always red.
	Blink Red	Upgrading software.
CONEXIÓN	Off	DSL link not established.
	Slow Blink Green	DSL line is training.
	Fast Blink Green	DSL interface is TX/RX packets.
	Green	DSL link established.
Internet	Off	No PPPoA or PPPoE connection
	Green	The PPPoA or PPPoE connection is established. The users can access the Internet.
	Red	Device attempts to become IP connected but fails (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)
Ethernet	Off	No Ethernet signal is detected.
	Blink Green	The user data is passing through Ethernet port.
	Green	Ethernet interface is ready to work
WLAN	Off	WLAN interface disable.
	Blink Green	WLAN interface is TX/RX packets.
	Green	WLAN interface enable.
WPS	Off	Off: WPS process is inactive
	Green	WPS process is on going

1.10.2 Rear Panel

The following table describes the interfaces and buttons of the router:

Interface	Description
ANT	Wireless antenna
ADSL	RJ-11 port, for connecting the router to the ADSL interface or a splitter via a telephone cable.
ETHERNET	RJ-45 port, for connecting the router to the Ethernet interface of a PC or other network devices via an Ethernet cable.
Power	Power interface, for connecting to the power adapter of 12 V, 800 mA.
RESET	Restore to the factory defaults. Keep the router powered on and push a needle into the hole for 10 seconds, then release it. The configuration is restored to the factory defaults.
○	Power switch, power on or power off the router.

2 Hardware Installation

The Router has three separate interfaces, an Ethernet LAN, a wireless LAN and an ADSL (WAN) interfaces. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it is exposed to moisture or excessive heat. Ensure that cables and the power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting.

2.1 Choosing the Best Location for Wireless Operation

Many environmental factors may affect the effective wireless function of the Router. If this is the first time that you set up a wireless network device, read the following information.

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting.

Designed to go up to 100 meters indoors and up to 300 meters outdoors, wireless LAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal range. Typical ranges vary depending on types of materials and background RF noise in your home or business. For optimum range and signal strength, use these basic guidelines.

- Keep the numbers of walls and ceilings to the minimum:
  The signal emitted from wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range of wireless LAN devices from 1 ~ 30 miters. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.
- Consider the direct line between access points and workstations:
  A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it appears over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90º angle) a wall or ceiling for better reception.
- Building materials make difference:
  Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signals can pass through drywall or open doorways. Avoid positioning them in the way that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.
- Position the antenna for best reception:
  Play around with the antenna position to see if signal strength improves. Some adapters or access points allow you to judge the strength of the signal.
- Keep your product away (at least 1~2 meters) from electrical devices:

- Keep wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

2.2 Connecting the ADSL Router

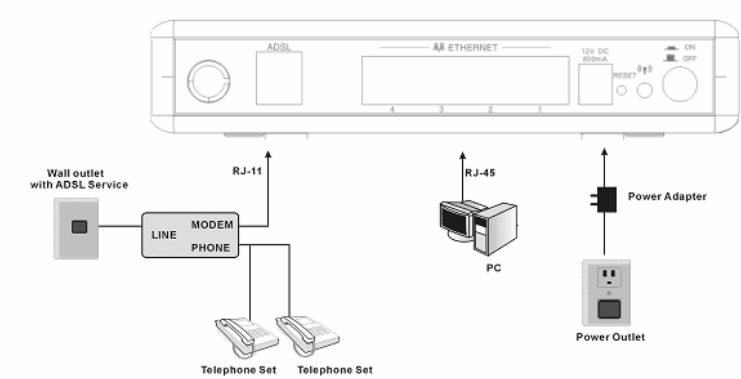
The following describes the procedure for connecting the Router with PC.

Step 1 Connect the **ADSL** interface of the Router through a telephone cable.

Step 2 Connect the **Ethernet** interface of the Router to the network card interface (NIC) of a PC through an Ethernet cable.

Step 3 Plug one end of the power adapter to the wall outlet and connect the other end to the **Powe**r interface of the Router.

The following figure displays the connection of the Router, PC, and telephones.



2.3 Factory Reset Button

The Router is reset to the factory default settings by pressing the RESET button for around 16 seconds while it is powered on. Use a ballpoint or paperclip to gently push down the RESET button. Remember that this operation may wipe out the settings stored in the flash memory, including user account information and LAN IP settings.

The factory configuration of the Router is as follows:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- User name: 1234
- Password: 1234

3 Introduction to Web Configuration

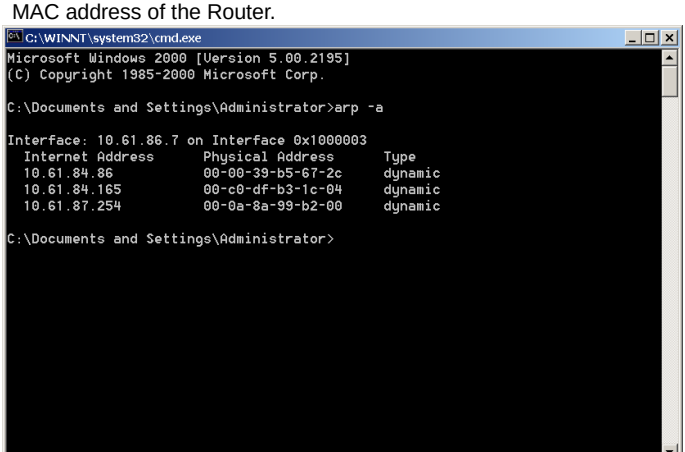
The first time you setup the Router. It is recommended that you configure the WAN connection using a single computer, to ensure that both the computer and the Router are not connected to the LAN. Once the WAN connection operates properly, you may continue to make changes to Router configuration, including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various menus used to configure and monitor the Router, including how to change IP settings and DHCP server setup.

3.1 Preparation before Login

Before accessing the Router, ensure the communication between PC and Router is normal. Check the communication between the PC and the Router as follows:

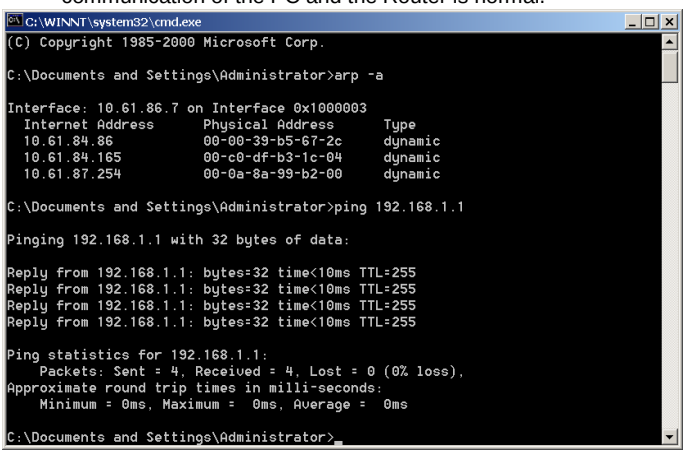
Step 4 Set the IP address of the PC to192.168.1.X (2~254), subnet mask to 255. 255.255.0, gateway address to 192. 168.1.1 (for a customized version, set them according to the actual version).

Step 5 Enter **arp -a** in the DoS window to check whether the PC can read the MAC address of the Router.



Step 6 Ping the management IP address (by default, it is 192.168.1.1) of the Router.

Step 7 If the PC can read the MAC address of the Router and can ping through the management IP address of the Router, which means the communication of the PC and the Router is normal.



Note:

When you manage the Router through Web, you must keep the Router power on. Otherwise, the Router may be damaged.

3.2 Logging In to the Router

The following description is a detail “How-To” user guide and is prepared for first time users.

3.2.1 First-Time Login

When you log in to the Router for the first time, the login wizard appears.

Step 1 Open a Web browser on your computer.

Step 2 Enter **http://192.168.1.1** (the Router default IP address) in the address bar. The login page appears.

Step 3 Enter the user name and password.

– The default username and password of the super user are **1234** and **1234**.

You need not enter the username and password again if you select the option **Remember my password**. It is recommended to change these default values after logging in to the Router for the first time.

Step 4 Click **OK** to log in or click **Cancel** to exit the login page.

After logging in to the Router as a super user, you can query, configure, and modify all settings. You can also diagnose the system.

You need to reboot the Router to enable your modification or configuration effective in some cases, for example, after you modify the PVC configuration. Some modification, such as adding a static route, takes effect at once, and does not require Router reboot.

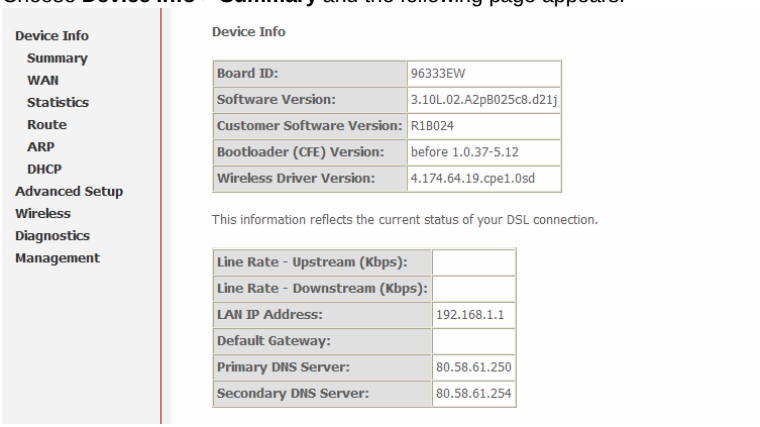
3.3 Device Info

Click **Device Info** and you can view the following information:

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP

3.3.1 Summary of Device Information

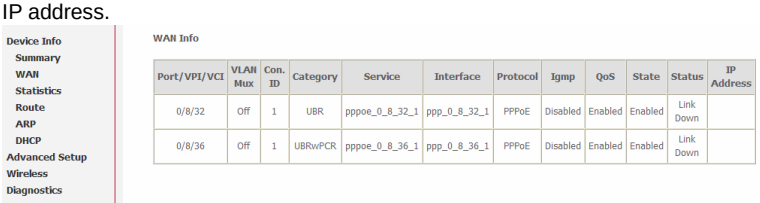
Choose **Device Info** > **Summary** and the following page appears.



- **LAN IP Address**: It displays the management IP address of the modem.
- **Default Gateway**: In the bridging mode, there is no gateway. In other modes, it is the IP address of the uplink equipment, for example, PPPoE, PPPoA.
- **DNS Server**: In the PPPoE / PPPoA mode, it is obtained from the uplink equipment. In the bridging mode, there is no DNS Server address and you can manually enter the information.

3.3.2 WAN Interface Information

Choose **Device Info** > **WAN** and the following page appears. The **WAN Info** page displays the detailed information of the PVC, including protocol, QoS, status, IP address.

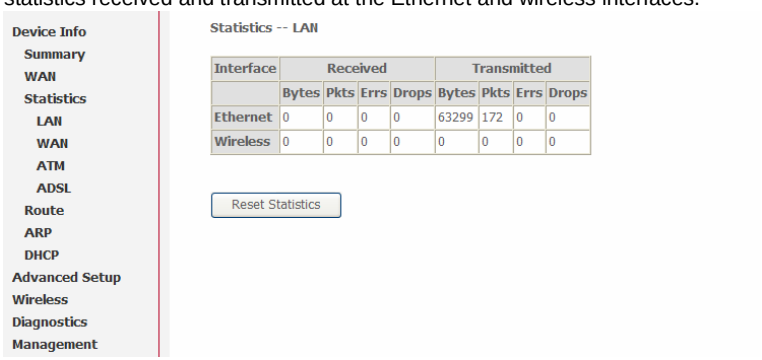


3.3.3 Statistics

Click **Statistics** and the **Statistics** page appears. It contains the following four items: **LAN**, **WAN**, **ATM**, and **ADSL**.

3.3.3.1 LAN

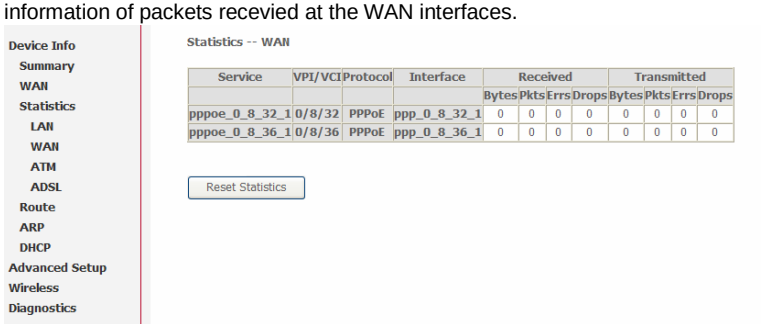
Choose **Statistics** > **LAN** and the following page appears. You can view the statistics received and transmitted at the Ethernet and wireless interfaces.



Click **Reset Statistics** to refresh the statistics of Ethernet and wireless interfaces.

3.3.3.2 WAN

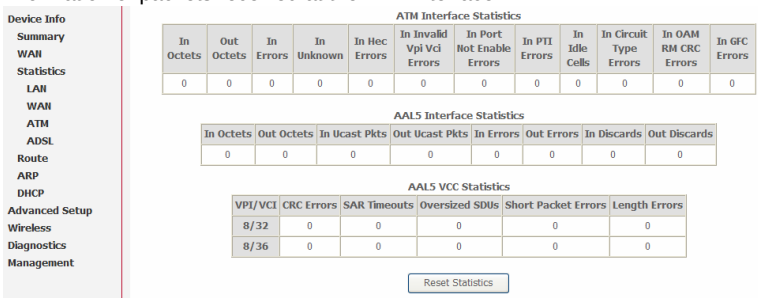
Choose **Statistics** > **WAN** and the following page appears. You can view information of packets recevied at the WAN interfaces.



Click **Reset Statistics** to refresh the statistics of WAN interfaces.

3.3.3.3 ATM

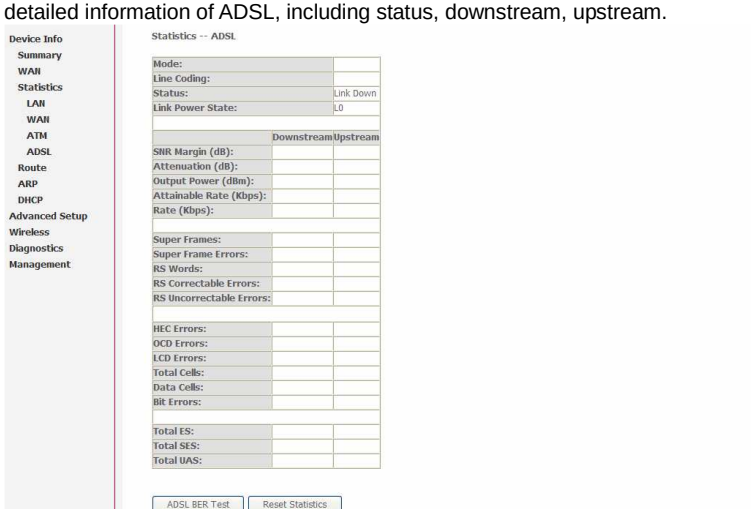
Choose **Statistics** > **ATM** and the following page appears. You can view information of packets recevied at the ATM interface.



Click **Reset Statistics** to refresh the statistics of ATM interfaces.

3.3.3.4 ADSL

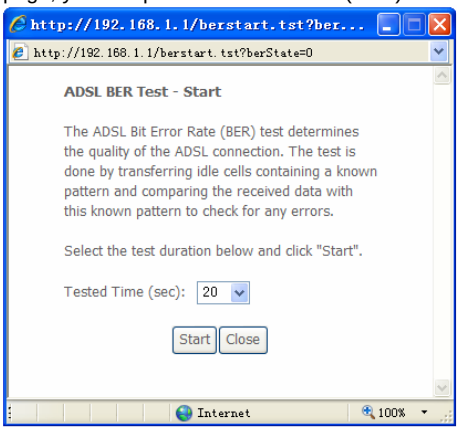
Choose **Statistics** > **ADSL** and the following page appears. You can view the detailed information of ADSL, including status, downstream, upstream.



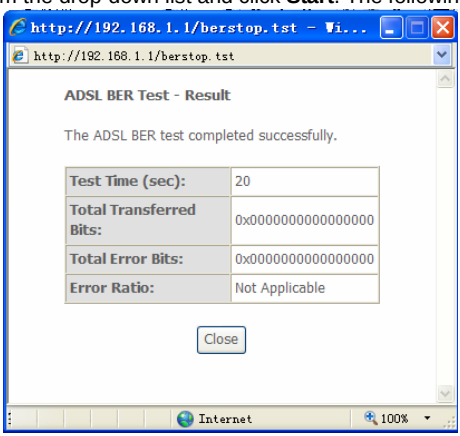
Click **Reset Statistics** at the bottom to restore the values to zero and recount them.

ADSL BER Test

Click **ADSL BER Test** in the **Statistics – ADSL** page and the following page appears. In this page, you can perform bit error rate (BER) test on the DSL line.



The **Tested Time (sec)** can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360. Choose the test time from the drop-down list and click **Start**. The following pages appear.

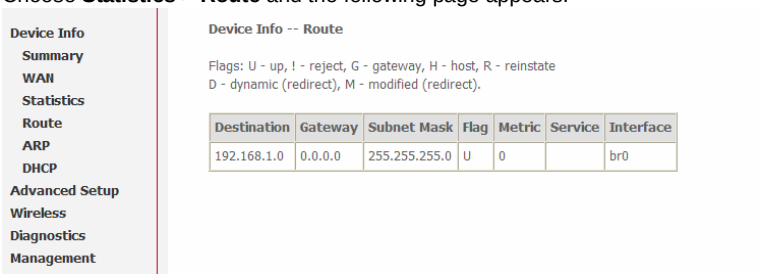


Note:

If the BER reaches e-5, you cannot access the Internet.

3.3.4 Route Table Information

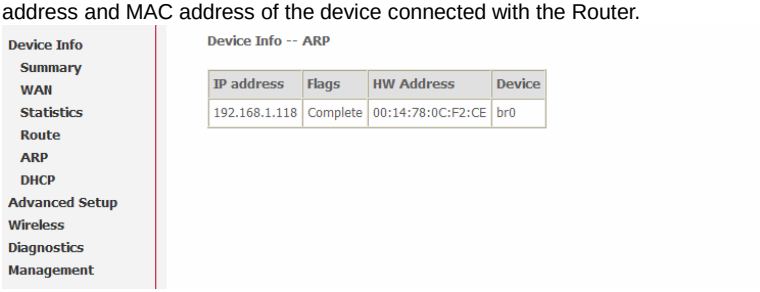
Choose **Statistics** > **Route** and the following page appears.



If the Router is set to PPPoE or PPPoA dial-up, the page is different.

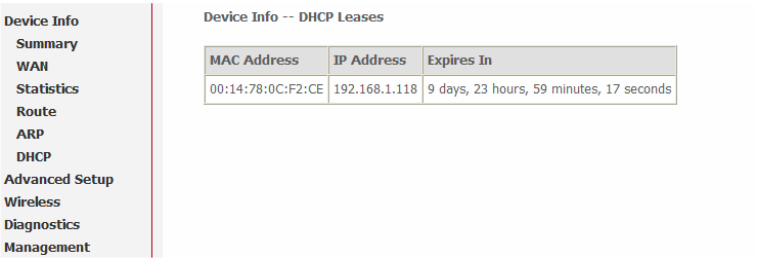
3.3.5 ARP Table Information

Choose **Statistics** > **ARP** and the following page appears. You can view the IP address and MAC address of the device connected with the Router.



3.3.6 DHCP

Choose **Statistics** > **DHCP** and the following page appears. You can view the MAC address and IP address of the device connected with the Router. The IP address of the connectd device is set to obtain the IP address automatically.



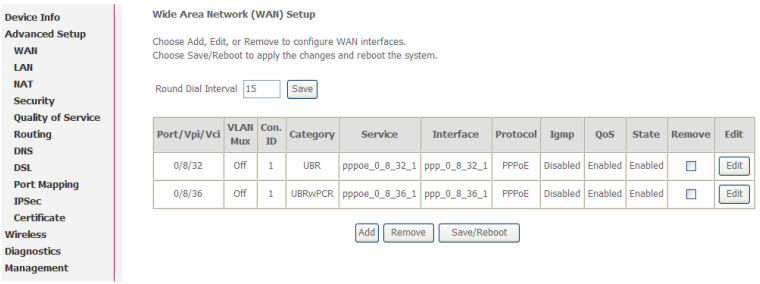
3.4 Advanced Setup

Click **Advanced Setup** and you can view the following information:

- WAN
- LAN
- NAT
- Security
- Quality of Service
- Routing
- DNS
- DSL
- Port Mapping
- IPSec
- Certificate

3.4.1 WAN Configuration

Choose **Advanced Setup > WAN** and the following page appears. In this page, you can view and configure the parameters of WAN.



Note:

If a PVC is deleted or modified, you need to reboot the Router. Otherwise, the modification does not take effect.

Click **Add**, **Edit**, or **Remove** to configure WAN interface.

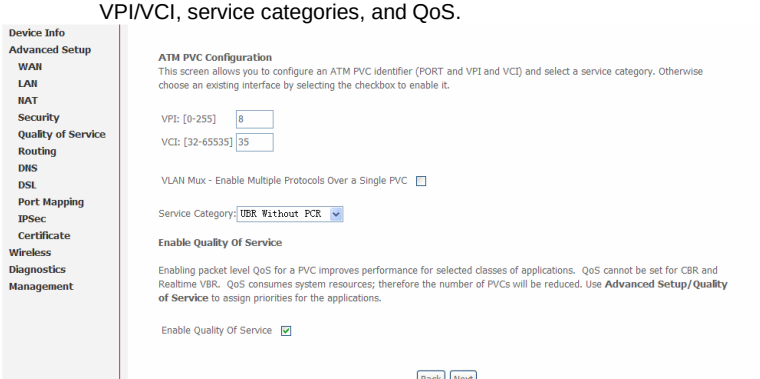
Click **Save/Reboot** to save the modification, and reboot the Router to make the modification effective.

The section shows you how to add PVC.

3.4.1.1 PPPoE Configuration

This section describes the procedure for adding PVC 8/35 (PPPoE mode).

Step 5 Click **Add** and the following page appears. In this page, you can modify VPI/VCI, service categories, and QoS.

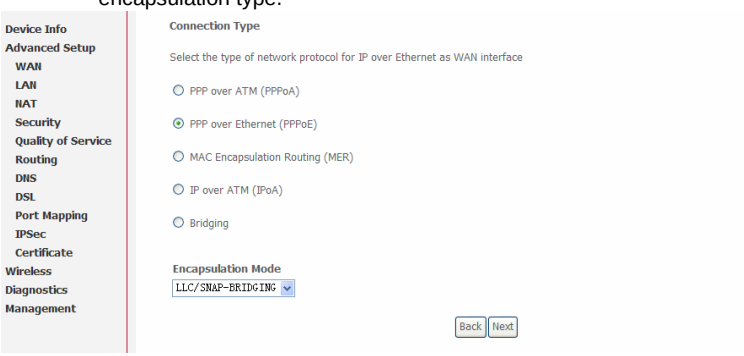


- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Service Category**: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.
- **Enable Quality Of Service**: Enable or disable QoS.

In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

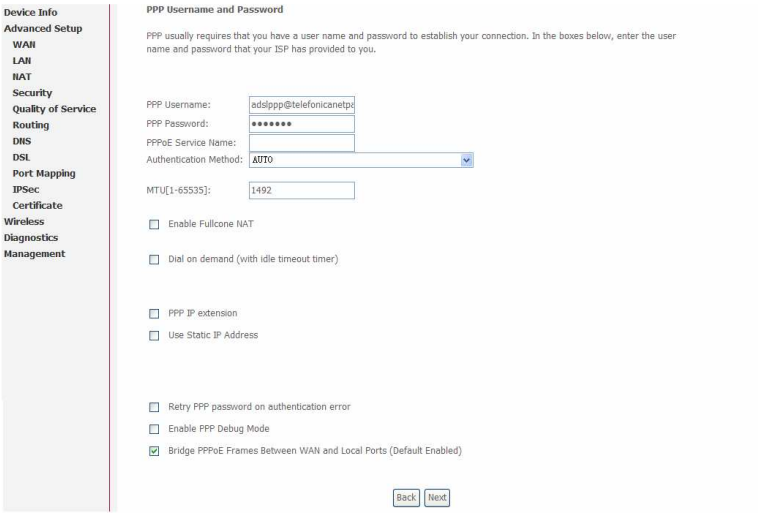
After proper modifications, click **Next** and the following page appears.

Step 6 In this page, you can modify the Internet connection type and encapsulation type.



Select the connection type of PVC 8/35 to **PPP over Ethernet (PPPoE)** and the encapsulation mode to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

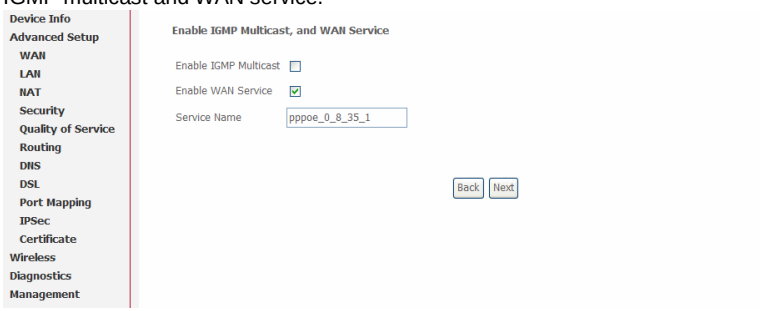
Step 7 In this page, you can modify the PPP user name, PPP password, authentication method, and other parameters.



- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** You can choose **AUTO**, **PAP**, **CHAP**, or **MSCHAP**. Usually, it is set to **AUTO**.
- **Dial on demand (with idle timeout timer):**
  - If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the Router does not detect the flow of the user continuously, the Router automatically stops the PPPOE connection. Once it detects the flow (like access to a webpage), the Router restarts the PPPOE dialup.
  - If this function is disabled, the Router performs PPPOE dial-up all the time. The PPPOE connnection does not stop, unless the Router is powered off and DSLAM or uplink equipment is abnormal.
- **PPP IP extension:** If this function is enabled, the WAN IP address obtained by the Router through built-in dial-up can be directly assigned to the PC being attached to the Router (at this time, the Router connects to only one PC). From the aspect of the PC user, the PC dials up to obtain an IP addres. But actually, the dial-up is done by the Router.

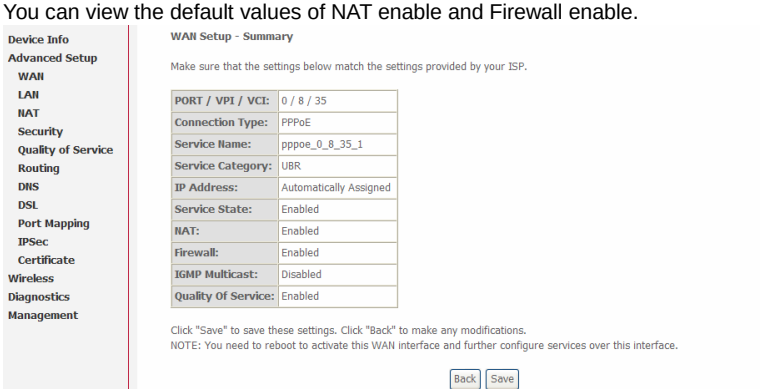
- If this function is disabled, the Router itself obtains the WAN IP address.
- **Use Static IP Address:** If this function is disabled, the Router obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up.If this function is enabled, the Router uses this IP address as the WAN IP address.

After entering the PPP user name and password, click **Next** and the following page appears. In this page, you can modify the service name, and enable or disable the IGMP multicast and WAN service.

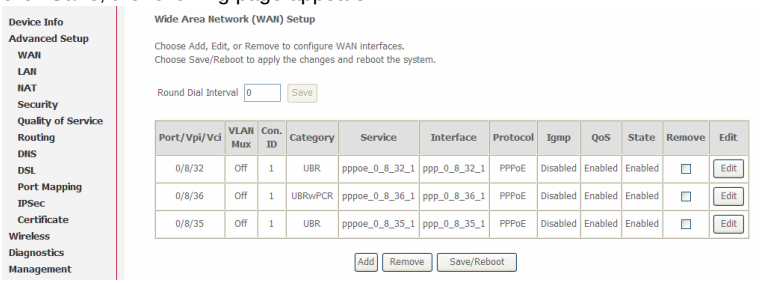


- **Enable IGMP Multicast**: IGMP proxy. For example, if you wish that the PPPoE mode supports IPTV, enable this function.
- **Enable WAN Service**: Enable it, unless you do not want to active the PVC.

Click **Nex**t and the following page appears. This page shows all the configuration. You can view the default values of NAT enable and Firewall enable.



Click **Save** to save the settings. Click **Back** to make any modifications. After you click **Save**, the following page appears.

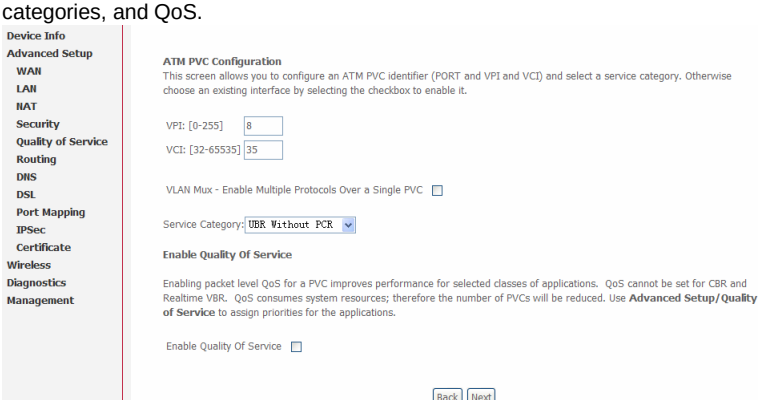


Note:

You need to reboot the Router to activate this WAN interface and further configure services in this page.

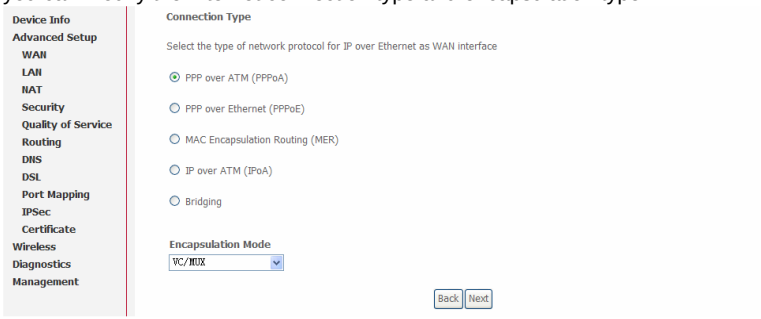
3.4.1.2 PPPoA Configuration

This section describes the procedure for adding PVC 8/35 (PPPoA mode). Click **Add** and the following page appears. In this page, you can modify VPI/VCI, service categories, and QoS.

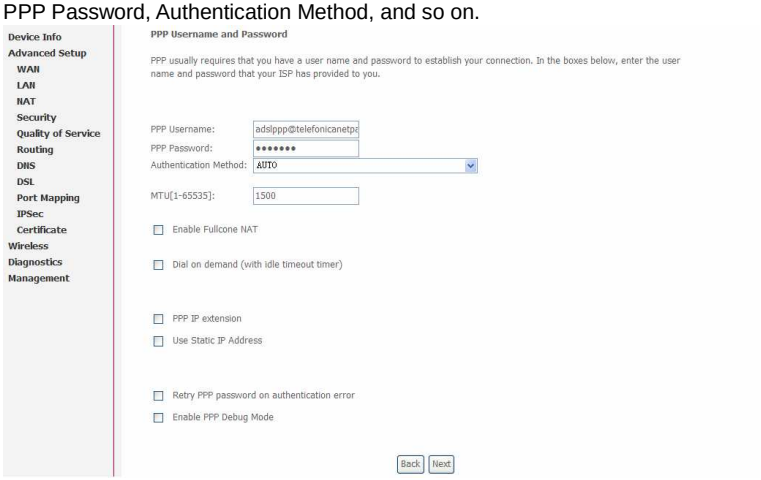


In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

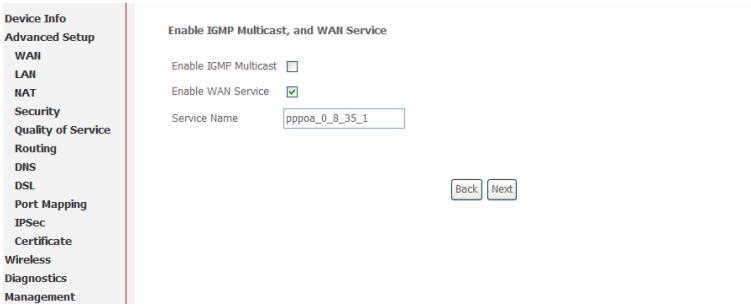
After proper modifications, click **Next** and the following page appears. In this page, you can modify the Internet connection type and encapsulation type.



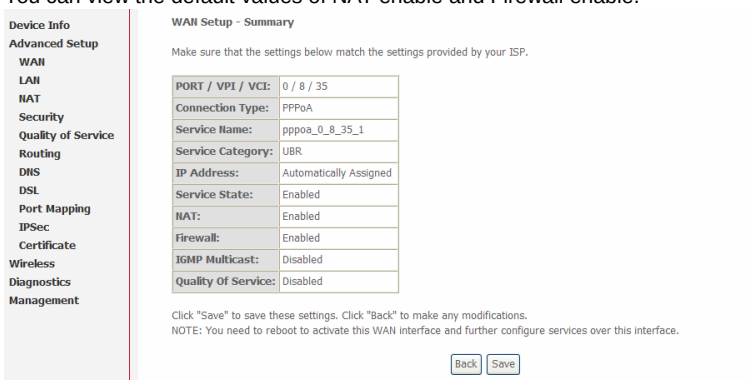
Set the connection type of PVC 8/35 to **PPP over ATM (PPPoA)** and encapsulation mode to **VC/MUX** (according to the uplink equipment). Click **Next** and the following page appears. In this page, you can modify the PPP Username, PPP Password, Authentication Method, and so on.



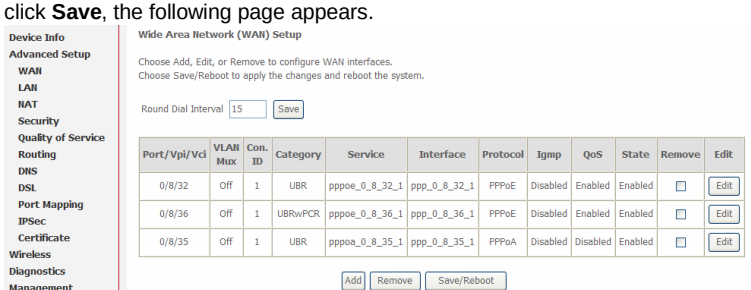
After entering the PPP user name and password, click **Next** and the following page appears. In this page, you can modify the service name, and enable or disable the IGMP multicast and WAN service.



Click **Next** and the following page appears. This page shows all the configuration. You can view the default values of NAT enable and Firewall enable.



Click **Save** to save the settings. Click **Back** to make any modifications. After you click **Save**, the following page appears.



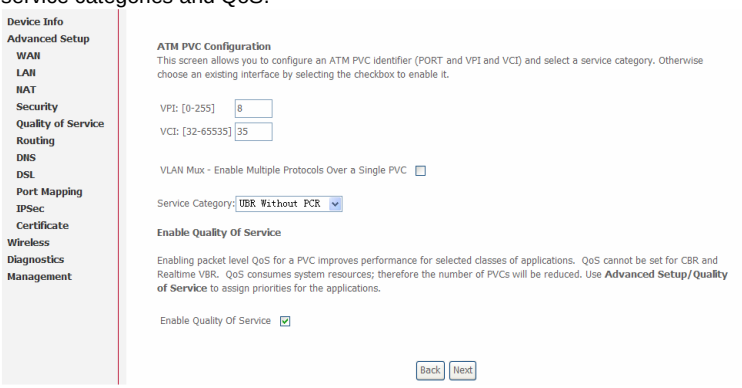
Note:

You need to reboot the Router to activate this WAN interface and further configure services in this page.

3.4.1.3 MER Configuration

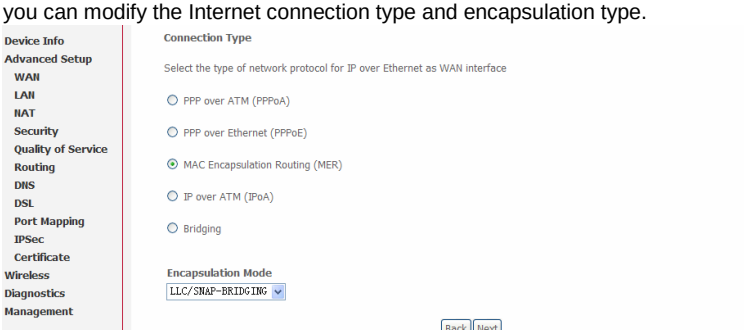
This section describes the procedure for adding PVC 8/35 (MER mode).

Click **Add** and the following page appears. In this page, you can modify VPI/VCIs, service categories and QoS.



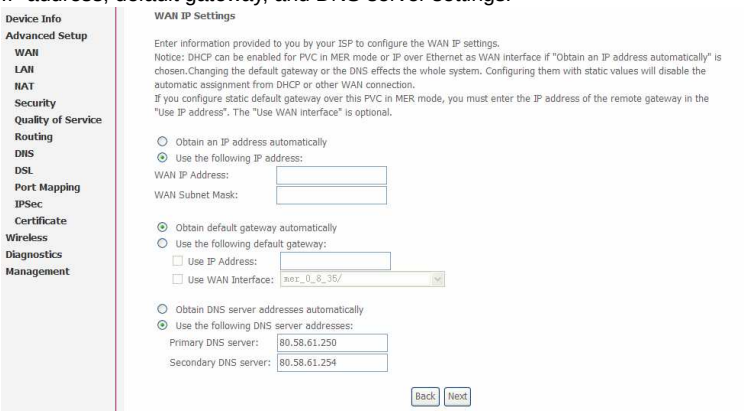
In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears. In this page, you can modify the Internet connection type and encapsulation type.



Set the connection type of PVC 8/35 to **MAC Encapsulation Routing (MER)** and encapsulation mode to **LLC/SNAP-BRIDGING** (according to the uplink equipment).

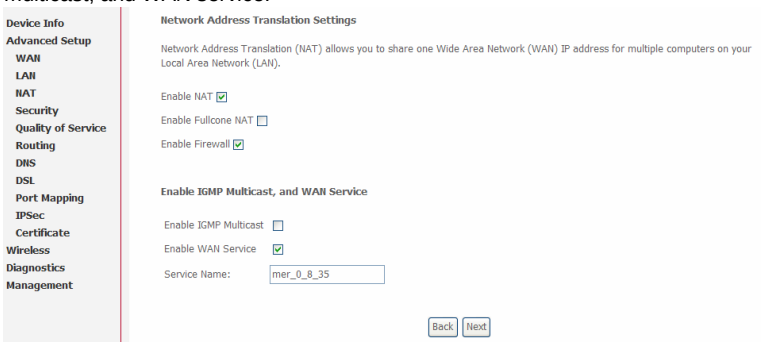
Click **Next** and the following page appears. In this page, you can modify the WAN IP address, default gateway, and DNS server settings.



- **Obtain an IP address automatically:** The Router obtains a (WAN) IP address automatically and at this time it enables DHCP client functions. The WAN IP address is obtained from the uplink equipment like BAS and the uplink equipment is required to enable the DHCP server functions.
- **Use the following IP address:** If you want to manually enter the WAN IP address, select this check box and enter the information in the field.
- **WAN IP Address:** Enter the IP address of the WAN interface provided by your ISP.
- **WAN Subnet Mask:** Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.
- **Obtain default gateway automatically:** Obtain the IP address of the default gateway assigned by the uplink equipment such as BAS.
- **Use the following default gateway:** If you want to manually enter the IP address of the default gateway, select this check box and enter the information in the fields.
- **Use IP Address:** Enter the gateway of the WAN interface provided by your ISP.

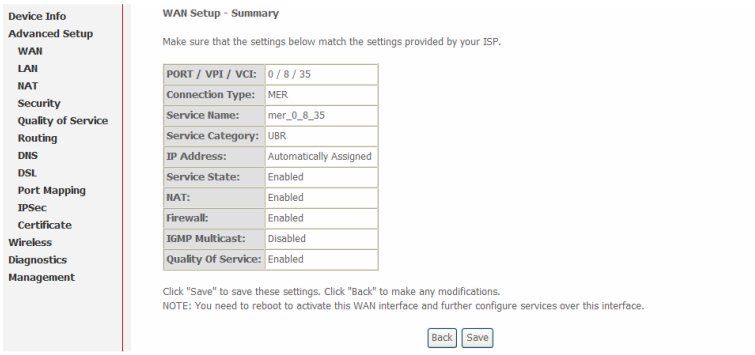
- **Use WAN Interface:** As to BAS equipment, it is the IP address of the downlink interface.
- **Obtain DNS server address automatically:** To obtain the IP address of the DNS server assigned by the uplink equipment such as BAS.
- **Use the following DNS server addresses:** If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.
- **Primary DNS server:** Enter the IP address of the primary DNS server.
- **Secondary DNS server:** Enter the IP address of the secondary DNS server provided by your ISP.

After proper modifications, click **Next** and the following page appears. In this page, you can modify the service name, and enable or disable the NAT, firewall, IGMP multicast, and WAN service.

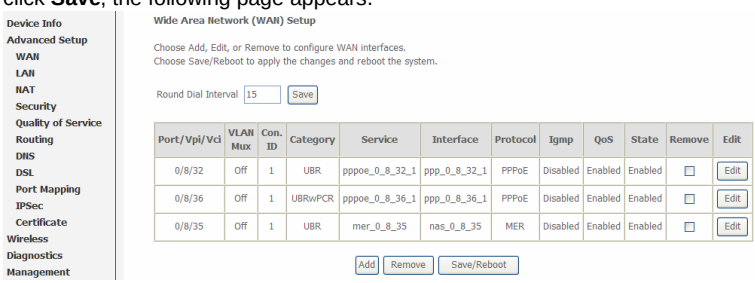


- **Enable NAT:** Select it to enable the NAT functions of the Router. If you do not want to enable NAT and wish the Router user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. It is normal to enable NAT.
- **Enable Firewall:** Enable or disable IP filtering.
- **Enable IGMP Multicast:** IGMP proxy. For example, if you wish that the MER mode supports IPTV, enable this function.
- **Enable WAN Service:** Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears. This page shows all the configuration.



Click **Save** to save the settings. Click **Back** to make any modifications. After you click **Save**, the following page appears.



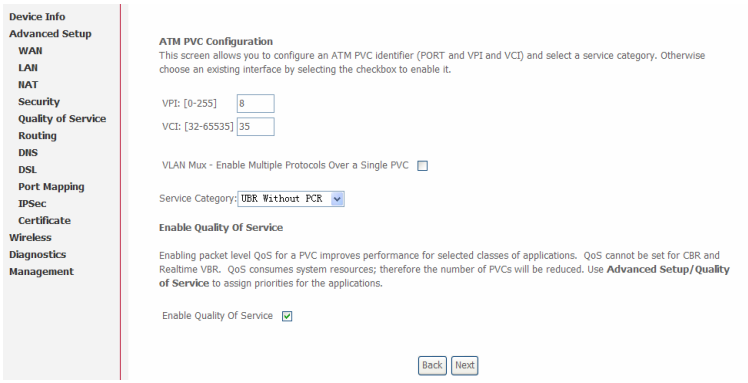
Note:

You need to reboot the Router to activate this WAN interface and further configure services in this page.

3.4.1.4 IPoA Configuration

This section describes the procedure for adding PVC 8/35 (IPoA mode).

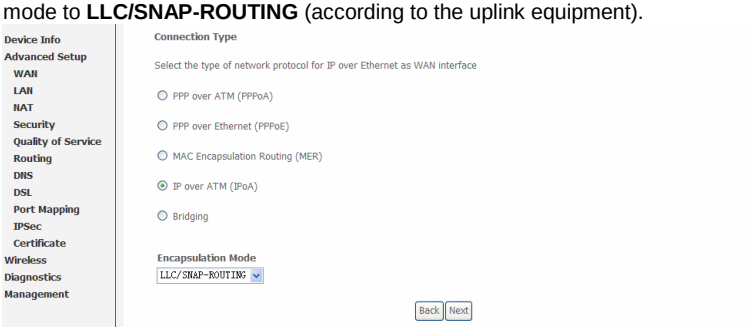
Click **Add** and the following page appears. In this page, you can modify VPI/VCIs, service categories, and QoS.



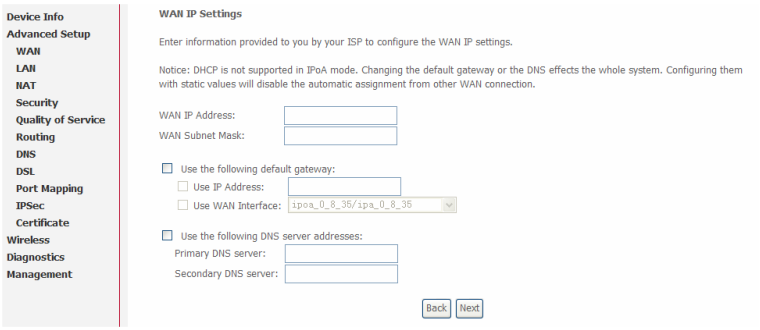
In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears. In this page, you can modify the Internet connection type and encapsulation type.

Set the connection type of PVC 8/35 to **IP over ATM (IPoA)** and the encapsulation mode to **LLC/SNAP-ROUTING** (according to the uplink equipment).

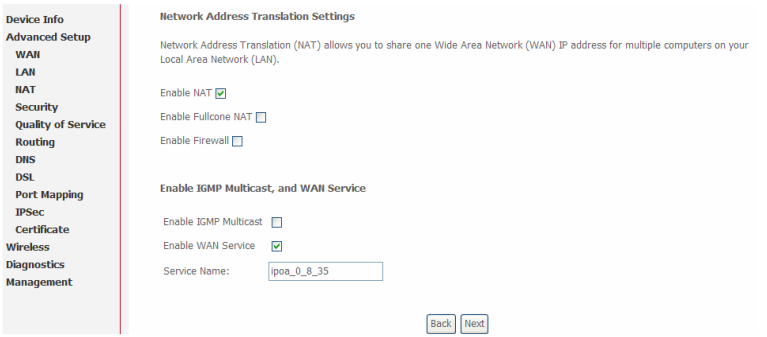


Click **Next** and the following page appears. In this page, you can modify the WAN IP, default gateway, and DNS server settings.



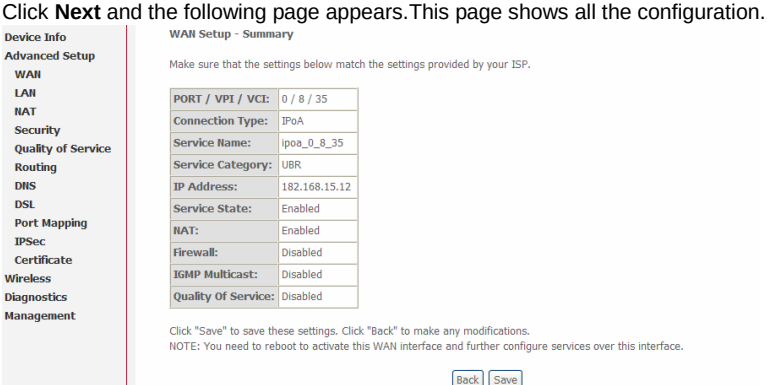
- **WAN IP Address:** Enter the IP address of the WAN interface provided by your ISP.
- **WAN Subnet Mask:** Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.
- **Use the following default gateway:** If you want to manually enter the IP address of the default gateway, select this check box and enter the information in the fields.
- **Use IP Address:** Enter the gateway of the WAN interface provided by your ISP.
- **Use WAN Interface:** As to BAS equipment, it is the IP address of the downlink interface.
- **Use the following DNS server addesses:** If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.
- **Primary DNS server:** Enter the IP address of the primary DNS server.
- **Secondary DNS server:** Enter the IP address of the secondary DNS server provided by your ISP.

After proper modifications, click **Next** and the following page appears. In this page, you can modify the service name, and enable or disable the NAT, firewall, IGMP multicast, and WAN service.

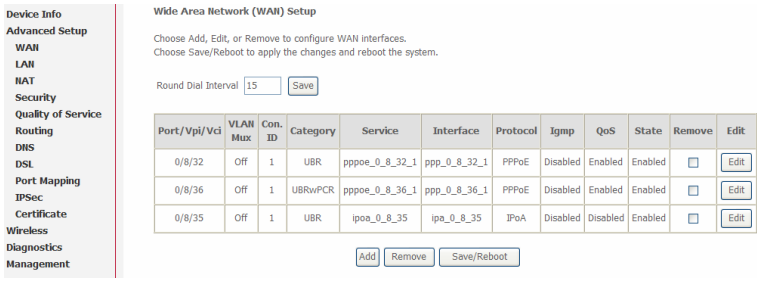


- **Enable NAT:** Select it to enable the NAT functions of the Router. If you do not want to enable NAT and wish the Router user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.
- **Enable Firewall:** Enable or disable IP filtering.
- **Enable IGMP Multicast:** IGMP proxy. For example, if you wish that the IPoA mode supports IPTV, enable this function.
- **Enable WAN Service:** Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears.This page shows all the configuration.



Click **Save** to save the settings. Click **Back** to make any modifications. After you click **Save**, the following page appears.



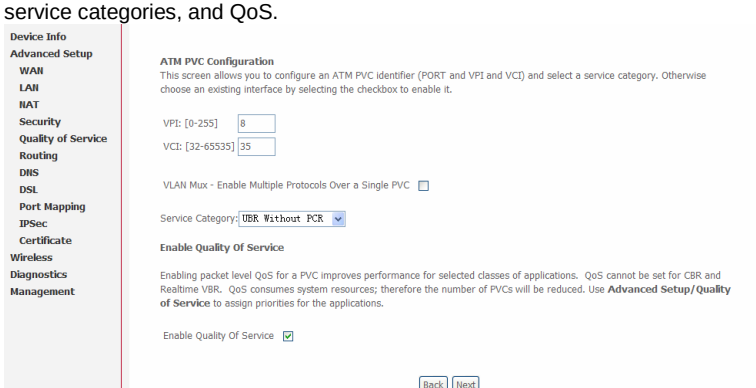
Note:

You need to reboot the Router to activate this WAN interface and further configure services in this page.

3.4.1.5 Bridge Configuration

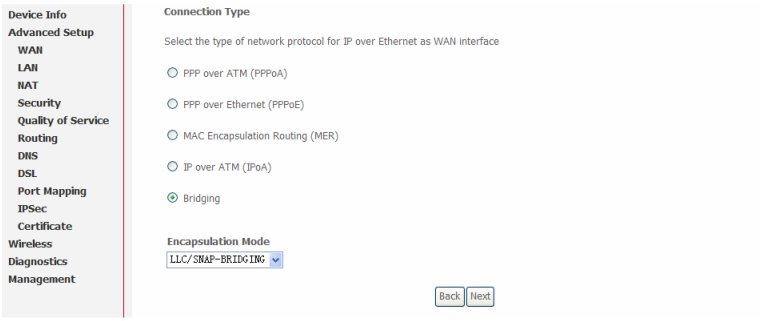
This section describes the procedure for adding PVC 8/35 (IPoA mode).

Click **Add,** and the following page appears. In this page, you can modify VPI/VCIs, service categories, and QoS.

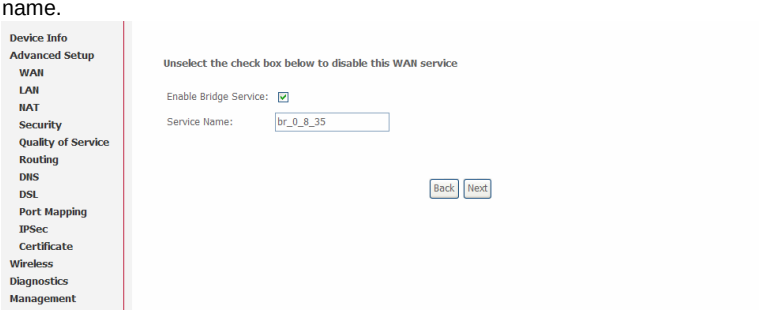


In this example, PVC 8/35 is to be modified and the default values of service category remain. In actual applications, you can modify them as required.

After proper modifications, click **Next** and the following page appears. In this page, you can modify the Internet connection type and encapsulation type.

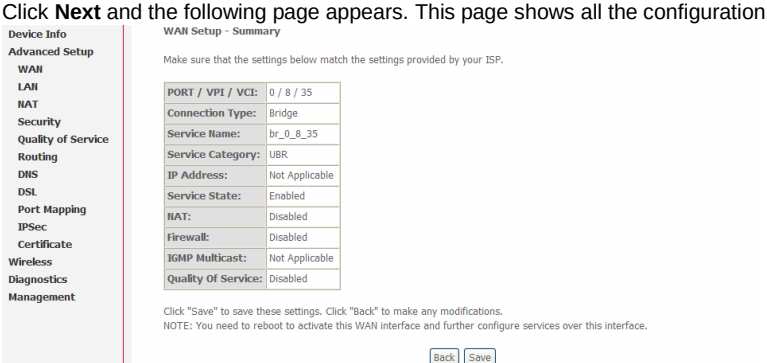


Click **Next** and the following page appears. In this page, you can modify the service name.

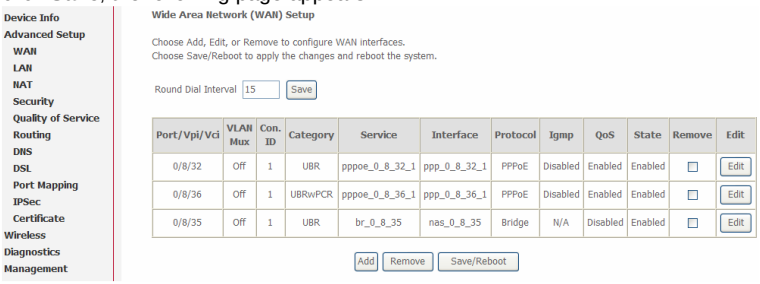


Enable Bridge Service: Enable it, unless you do not want to active the PVC.

Click **Next** and the following page appears. This page shows all the configuration.



Click **Save** to save the settings. Click **Back** to make any modifications. After you click **Save**, the following page appears.

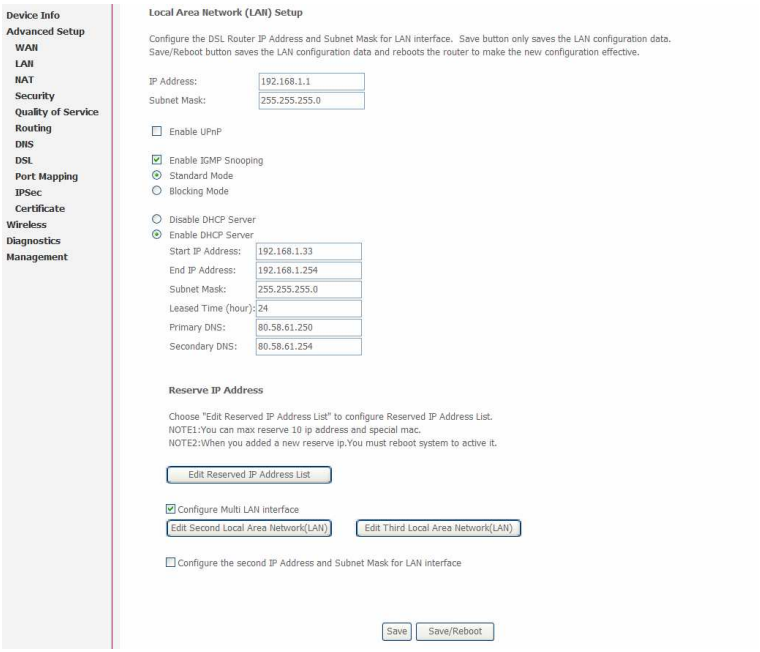


Note:

You need to reboot the Router to activate this WAN interface and further configure services in this page.

3.4.2 LAN Configuration

Choose **Advanced Setup** > **LAN** and the following page appears. In this page, you can modify and configure IP Address and DHCP Server.



3.4.3 NAT

Click **NAT** and the **NAT** page appears. It contains the following three items: **Virtual Servers**, **Port Trigger**, and **DMZ Host**.

3.4.3.1 Overview

Setting up the NAT Function

- The Router is equipped with the network address translation (NAT) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the public IP address of the router by default.
- One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it is explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in

the local network, and so the router allows the data to pass through. The router opens one specific port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).

- If an external application tries to send a call to a PC in the local network, the router blocks it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links (that is. several ports), so that players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot run if NAT is activated.
- Using port forwarding (the forwarding of requests to particular ports), the router is forced to send requests from the Internet for a certain service, for example, a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the Router forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service. Where configuration is concerned, you must define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger port, then it opens the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it to pass through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

Note:

- An application that is configured for port triggering can only be run by one user in the local network at a time.

- After public ports are opened, they can be used by unauthorized persons to gain access to a PC in the local network.
- When the Router is supplied, the NAT function is activated. For example, all IP addresses of PCs in the local network are converted to the public IP address of the router when accessing the Internet. You can use NAT settings to configure the Router to carry out the following tasks.
- For functions described as follows, IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the Router, you must disable DHCP server as the settings in the local network menu entry for the lease time or assign static IP addresses for the PCs.

You can enable or disenable the NAT function. By default, the NAT function is enabled.

3.4.3.2 NAT-Virtual Server Setup

By default, Router blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude into the network and damage it.

However, you may want to expose your network to the Internet in limited and controlled ways in order to enable some applications to work from the LAN (for example, game, voice, and chat applications) and to enable Internet access to servers in the home network. The port forwarding feature supports both functionalities. This topic is also referred as Local Servers.

The port forwarding page is used to define applications that require special handling by Router. All you need to do is to select the application protocol and the local IP address of the computer that is using or providing the service. If required, you may add new protocols in addition to the most common ones provided by Router.

For example, if you wanted to use a file transfer protocol (FTP) application on one of your PCs, you would simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at Router from the Internet henceforth is forwarded to the specific computer.

Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that provide it. This is useful, for example, if you want to host a Web server inside your home network.

When an Internet user points his/her browser to Router external IP address, the gateway forwards the incoming HTTP request to your Web server. With one external IP address (Router main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer.

For example, you can define that FTP uses address X to reach computer A and Telnet also uses address X to reach computer A. But attempting to define FTP to use address X to reach both computer A and B fails. Router, therefore, provides the ability to add additional public IP addresses to port forwarding rules, which you must obtain from your ISP, and enter into the IP addresses pool. Then, you can define FTP to use address X to reach computer A and address Y to reach computer B.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. For example, if you have a Web server running on your PC on port 8080 and you want to grant access to this server to any one who accesses Router via HTTP.

To accomplish this, do as follows:

Step 1 Define a port forwarding rule for the HTTP service, with the PC IP or host name.

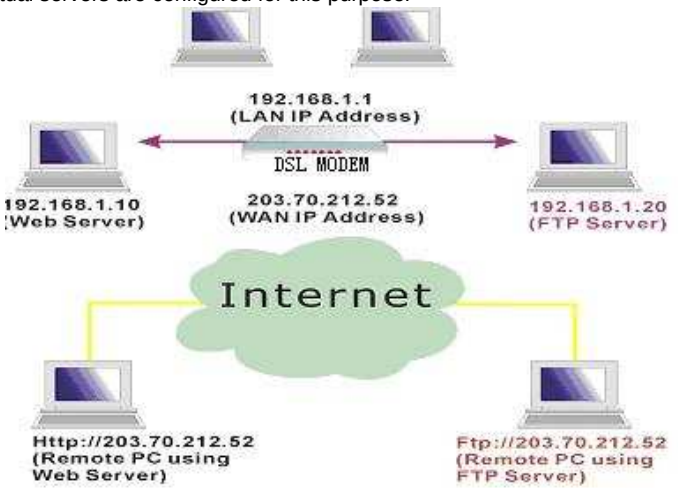
Step 2 Specify 8080 in the **Forward to Port** field.

All incoming HTTP traffic is forwarded to the PC running the Web server on port 8080. When setting a port forwarding service, ensure that the port is not used by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP, the port used by the gateway VoIP application (5060) is the same port, on which port forwarding is set for LAN SIP agents.

Note:

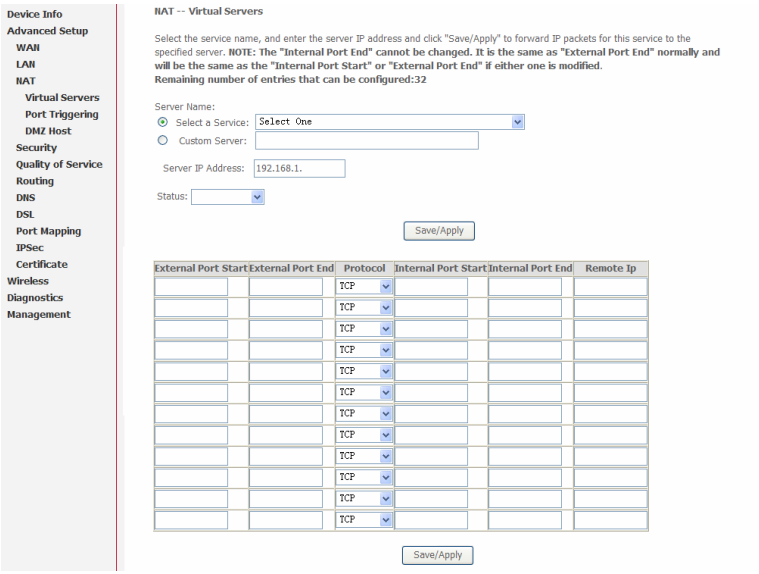
Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific application level gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. Router is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network. The ALG is automatically assigned based on the destination port.

Virtual servers are configured for this purpose.



Adding Port Forwarding

Step 1 Choose **NAT** > **Virtual Servers** and the **NAT-Virtual Servers** page appears. In this page, click **Add** and the following page appears.



- Server Name: You can select a service from the drop-down list or enter a custom server.
- Server IP Address: Enter the server IP address of the computer that provides the service (the server in the local host field). Note that unless an additional external IP address is added, only one LAN computer can be assigned to provide a specific service or application.
- Protocol: You can select **TCP**, **UDP**, or TCP/UDP from the drop-down list.

If the application you require is not in the list, enter the information manually.

Select the protocol from the drop-down list for the service you provide.

In the **External Port** filed, enter the port number of the service you provide.

In the **Internal Port** field, enter the internal port number, to which service requests are to be forwarded.

In the **Local IP Address** field, enter the IP address of the PC that provides the service.

Example

The Web server is configured to react to requests on port 8080. However, the requests from websites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port

8080 as an internal port, all requests from the Internet are diverted to the service with port 80 on the Web server of the PC you have defined with port 8080.

Deleting Port Forwarding

Step 1 Select the Remove check box.

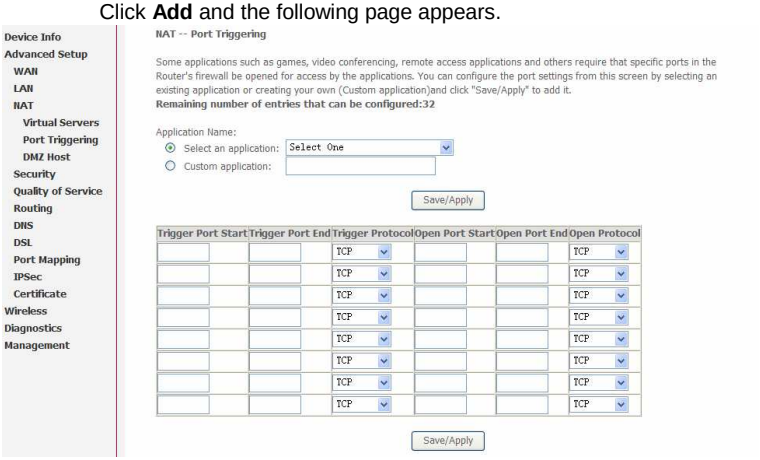
Step 2 Click Remove to apply the settings.

3.4.3.3 Port Triggering

If you configure port triggering for a certain application, you need to determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or manually assign ports or port blocks.

Adding Port Triggering

Step 1 Choose **NAT**> **Port Trigger** and the **Port Trigger Setup** page appears. Click **Add** and the following page appears.



Step 2 Select the required application from the **Select an application** drop-down list, or manually enter the information in the **Custom application** field.

- **Trigger Port Start** and **Trigger Port End**: enter the port that is to be monitored for outgoing data traffic.
- **Trigger Protocol**: select the protocol that is to be monitored for outgoing data traffic.

- **Open Port Start** and **Open Port End**: enter the port that is to be opened for incoming traffic.
- **Open Protocol**: select the protocol that is to be allowed for incoming data traffic

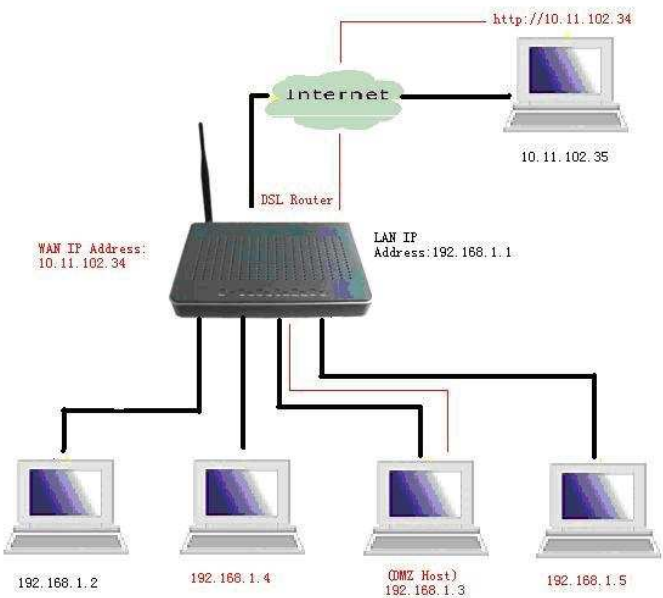
Step 3 Click **Save/Apply** to apply the settings.

Removing Port Triggering

Step 1 Select the **Remove** check box.

Step 2 Click **Save/Apply** to apply the settings.

3.4.3.4 DMZ Host



The demilitarized military zone (DMZ) host feature allows one local computer to be exposed to the Internet. This function is applicable for:

- Users who want to use a special-purpose Internet service, such as an on-line game or video conferencing program, that is not presented in the port forwarding list and for which no port range information is available.
- Users who are not concerned with security and wish to expose one computer to all services without restriction.

Note:

A DMZ host is not protected by the firewall and may be vulnerable to attack. This may also put other computers in the home network at risk. Hence, when designating a DMZ host, you must consider the security implications and protect it if necessary.

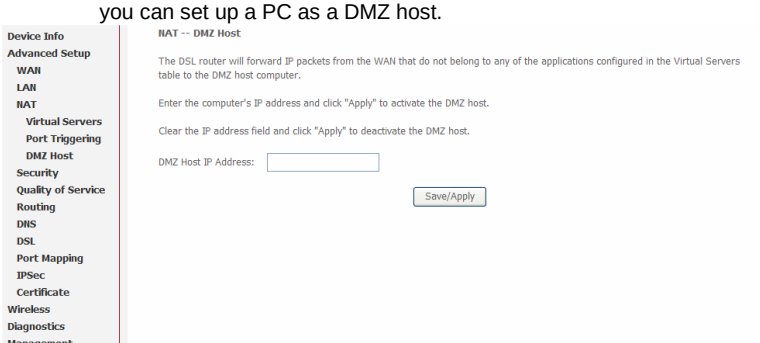
You can set up a client in your local network as a so-called DMZ host. Your device then forwards all incoming data traffic from the Internet to this client. You can, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (for example, hacker attacks). Enable this function only when necessary (for example, to operate a Web server) and when other functions (for example, port forwarding) are inadequate. In this case, you should take appropriate measures for the clients concerned.

Note:

Only one PC per public IP address can be set up as an exposed host.

Adding a DMZ host

Step 1 Choose **NAT** > **DMZ Hos**t and the following page appears. In this page, you can set up a PC as a DMZ host.



Step 2 Enter the local IP address of the PC that is to be enabled as an exposed host.

Step 3 Click Save/Apply to apply the settings.

Remove DMZ host

Step 1 Clear the DMZ host address.

Step 2 Click **Save/Apply** to apply the settings.

3.4.4 Security

Click **Security** and the **Security** page appears. It contains the following three items: **IP Filter**, **Parental Control**, and **Url Filter**.

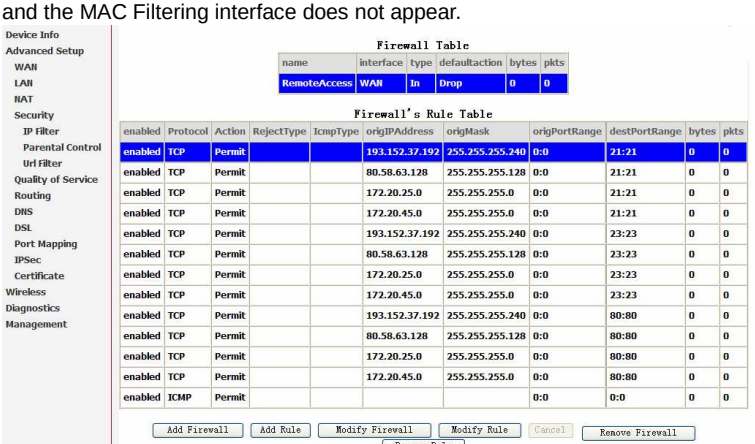
3.4.4.1 IP Filter

Choose **Security** > **IP Filter** and the following interface appears. By default, the firewall is enabled. The firewall is used to block document transmissions between the Internet and your PC. It serves as a safety guard and permits only authorized documents to be sent to the LAN.

Note:

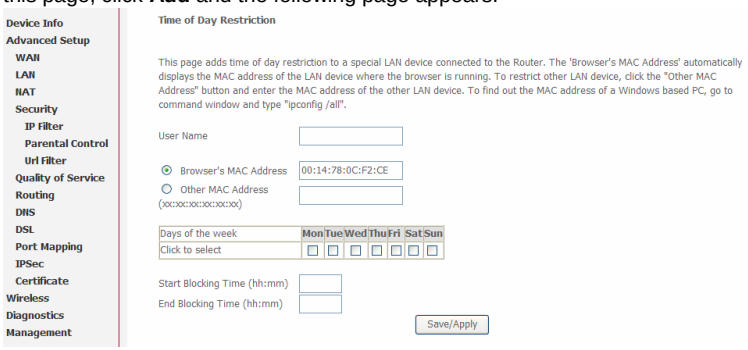
If the Router is configured to bridge mode only, IP filtering is disabled and the IP filtering interface does not appear.

If the Router does not configure a PVC of Bridge mode, MAC filtering is disabled and the MAC Filtering interface does not appear.



3.4.4.2 Parental Control

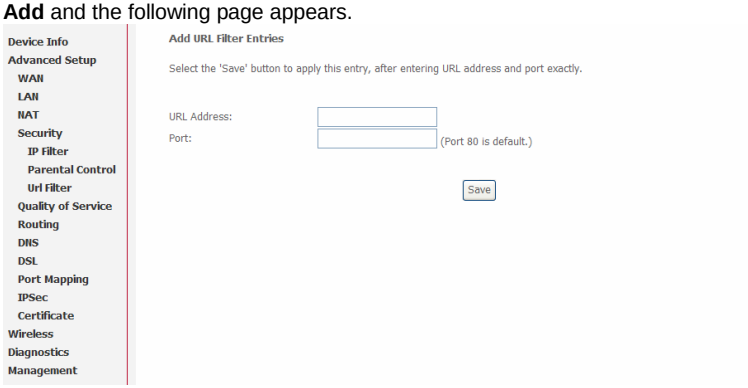
Choose **Security** > **Parental Control** and the **Parental Control** page appears. In this page, click **Add** and the following page appears.



In this page, you can add time of day restriction to a special LAN device connected to the Router. The **Browser's MAC Address** automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click **Other MAC Address** and enter the MAC address of the another LAN device. To obtain the MAC address of a Windows based PC, enter **ipconfig /all** in the DoS window.

3.4.4.3 Url Filter

Choose **Security** > **Url Filter** and the **URL Filter** page appears. In this page, click **Add** and the following page appears.



- **URL Address**: Enter the IP address of the URL.
- **Port**: Enter the port. By default, it is the port 80.

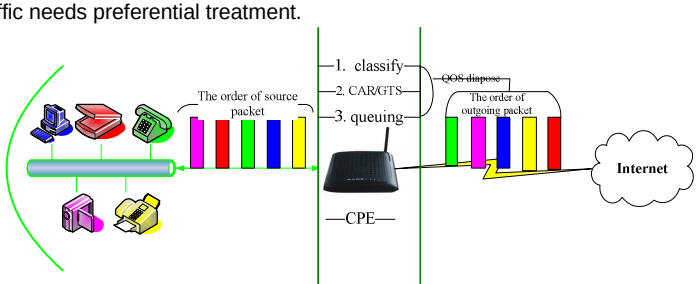
3.4.5 Quality of Service

Click **Quality of Service** and the **Quality of Service** page appears. It contains the following two items: **Queue Config** and **QoS Classification**.

Many communication and multimedia applications require large, high-speed bandwidths to transfer data between the local network and the internet. However, for many applications there is often only one internet connection available with limited capacity. QoS divides this capacity between the different applications and provides undelayed, continuous data transfer in situation where data packets with higher priority are given preference.

Network QoS is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

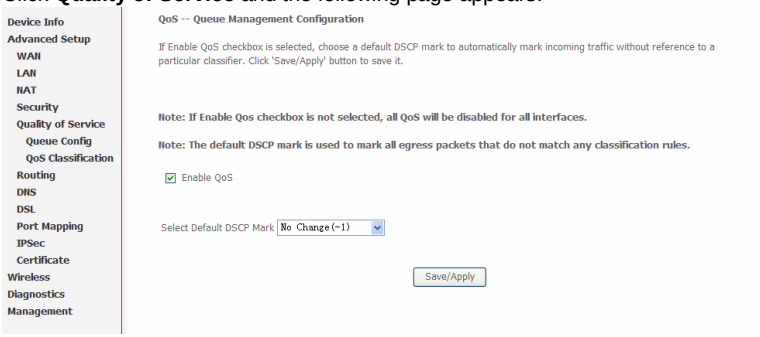
Traditionally, the concept of quality in networks meant that all network traffic was treated equally. The result was that all network traffic received the network's best effort, with no guarantees for reliability, delay, variation in delay, or other performance characteristics. With best-effort delivery service, however, a single bandwidth-intensive application can result in poor or unacceptable performance for all applications. The QoS concept of quality is one in which the requirements of some applications and users are more critical than others, which means that some traffic needs preferential treatment.



3.4.5.1 Enabling QoS

In this page, you can perform QoS queue management configuration. By default, the system enables QoS and sets a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.

Click **Quality of Service** and the following page appears.



Select **Enable QoS** to enable QoS and set the default DSCP mark.

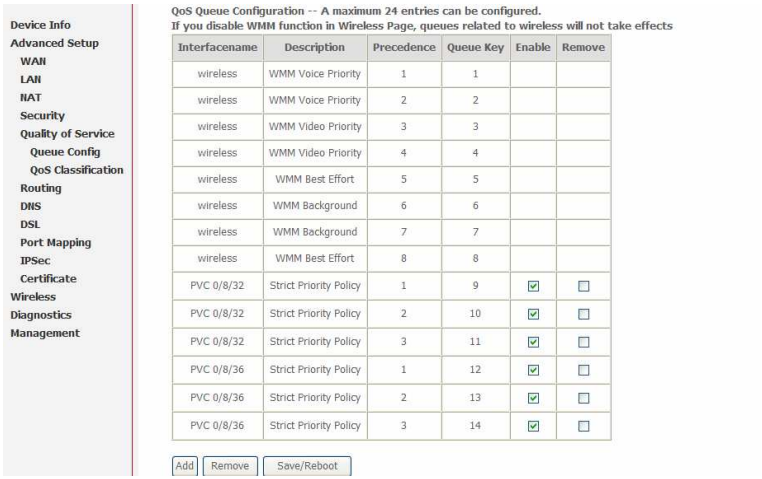
Click **Save/Apply** to apply the settings.

3.4.5.2 QoS-Queue Configuration

Choose **Quality of Service** > **Queue Configure** and the following page appears. In this page, you can configure QoS queue. A maximum of 24 entries can be configured.

The queuing in packet QoS becomes effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging, not under control of the packet QoS.

QoS Queue Configuration can allocate four queues. Each of the queues can be configured for a precedence value (Lower integer values for precedence imply higher priority for this queue relative to others). The queue entry configured is used by the classifier to place ingress packets appropriately.

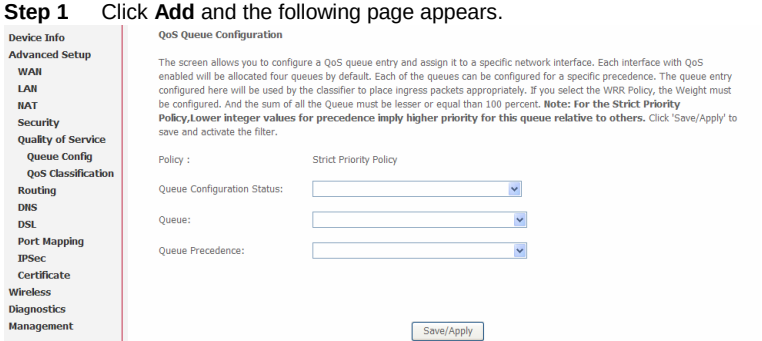


Note:

Lower integer values for precedence imply higher priority for this queue relative to others.

For example, add a QoS queue entry and allocate it to a specific network interface (PVC 0/8/32). Set integer values for queue precedence to 1.

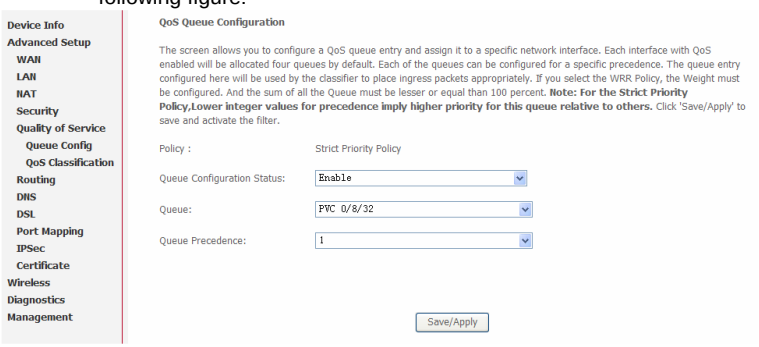
Step 1 Click **Add** and the following page appears.



- **Policy Select**: It displays **Strict Priority Policy**.
- **Queue Configuration Status**: set to enable or disable a QoS queue.

- **Queue**: select a specific network interface. When you have already selected a network interface, the specific network interface selected automatically allocates to the queue.
- **Queue Precedence**: select an integer value for queue precedence. After you select an integer value, the queue entry appropriately places to ingress packets. Lower integer values for precedence imply higher priority for this queue relative to others.

Step 2 Add a QoS queue entry and assign it to a specific network interface (PVC 0/0/35), and set integer values for queue precedence to 1. See the following figure:

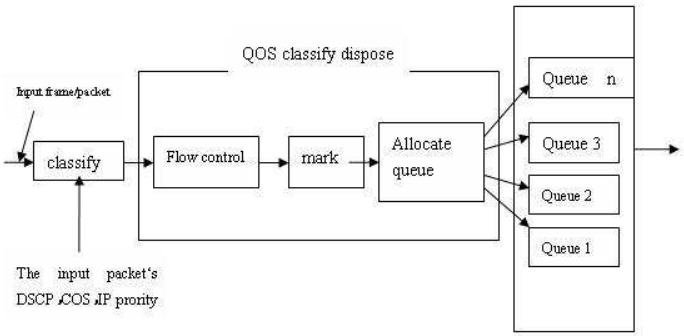


Step 3 After setting, click **Save/Apply** and the following page appears. This configuration takes effective at once.

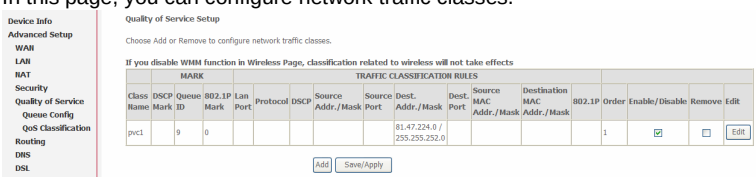
To delete a certain queue, disable it, select it, and then click **Remove**.

3.4.5.3 QoS-QoS Classification

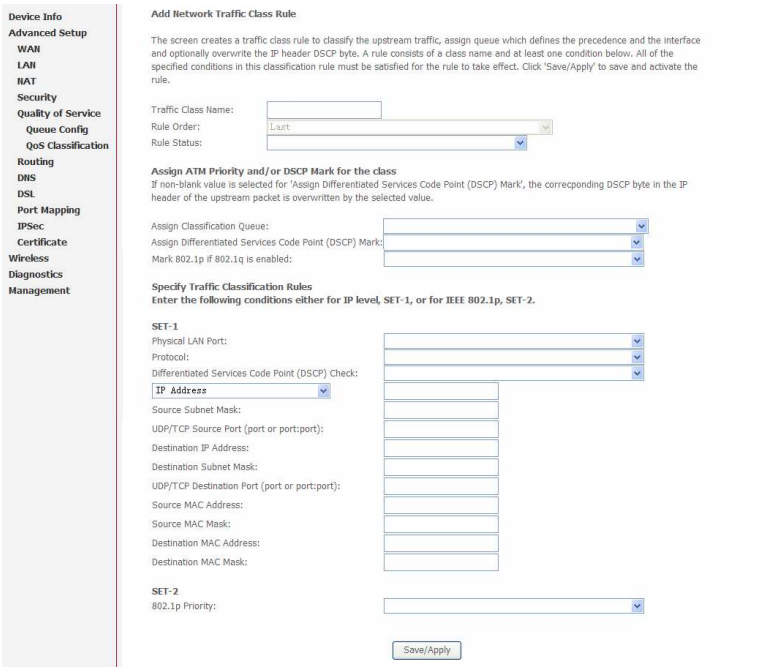
Some applications require specific bandwidth to ensure its data be forwarded in time. QoS classification can creates traffic class rule to classify the upstream traffic. Assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. After QoS classification, QoS divides capacity between different applications and provides undelayed, continuous data transfer where data packet with higher priority is given preference. The follow figure shows QoS classification.



Choose **Quality of Service** > **QoS Classification** and the following page appears. In this page, you can configure network traffic classes.



Click **Add** and the following page appears.



- **Traffic Class Name:** Enter a name of the class.
- **Rule Order:** Select order for queue.
- **Rule Status:** Enable or disable this traffic class rule.
- **Assign Classification Queue:** Select a classification queue.
- **Assign Differentiated Service Code Point (DSCP) Mark:** Select a mark service that modifies the original packet IP header if all rules defined within the classification class are matched. (CS-Mark IP Precedence, AF-Assured Forwarding, EF-Expedited Forwarding)
- **Mark 802.1p if 802.1q is enabled:** Select an 802.1p priority number that serves as the 802.1p value.

There are two sets of classification rules. Set-1 is based on different fields within TCP/UDP/IP layer plus physical LAN port; Set-2 is based on MAC layer IEEE 802.1p priority field.

Set-1 Rules contain the following:

- Physical LAN Port: Select one among USB port, Ethernet ports and wireless port.
- Protocol: Select one among TCP/UDP TCP UDP or ICMP protocols.
- Source IP Address
- Source subnet mask
- UPD/TCP Source Port
- Destination IP Address
- Destination Subnet Mask
- UPD/TCP destination port or a range of ports
- Source Mac Address
- Source Mac Mask
- Destination Mac Address
- Destination Mac Mask

Set-2 Rules contain the following:

802.1p Priority: the 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one.

QoS-DSCP Setting

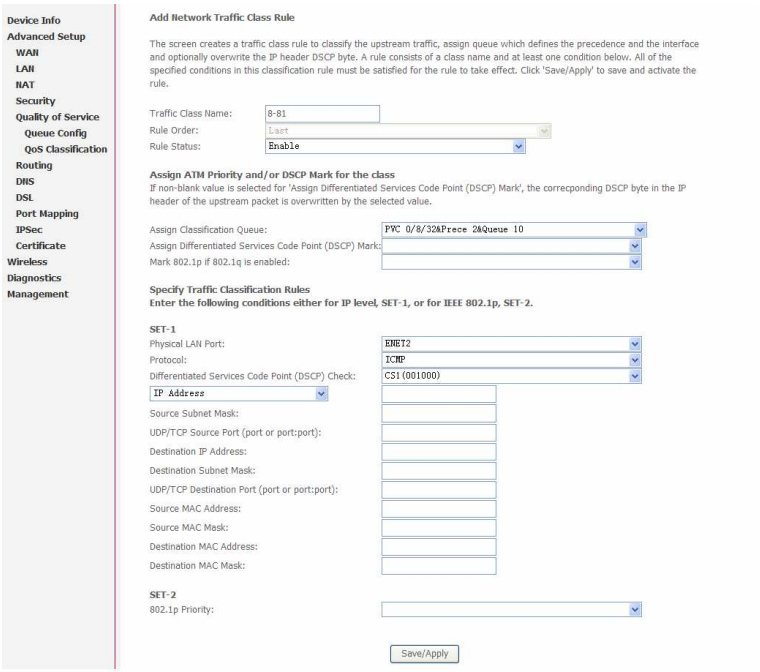
In order to understand what is differentiated services code point (DSCP), you should be familiar with the differentiated services model (Diffserv).

Diffserv is a class of service (CoS) model that enhances best-effort Internet services via differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service,

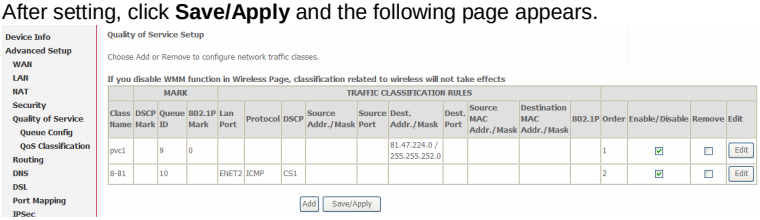
via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

As displayed in following diagram, the IPV4 packet has a TOS filed. Diffserv defines TOS field in IP packet headers referred to as DSCP. Hosts or routes that pass traffic to a Diffserv-enabled network typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handing or scheduling behavior.

For example, mark each transmitted ICMP packet which passes traffic to 0-35class with an appropriate DSCP (CS1).



After setting, click **Save/Apply** and the following page appears.



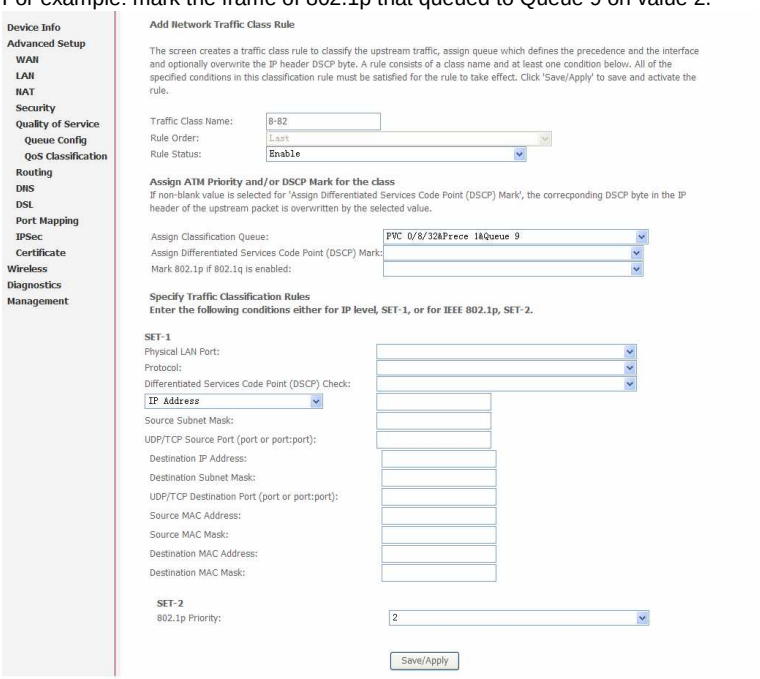
Click **Save/Apply**. This configuration takes effective at once.

QoS-802.1p Setting

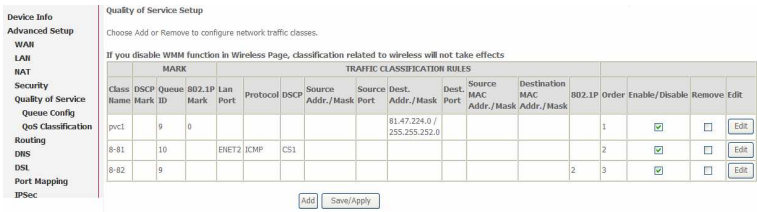
The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The follow diagram shows the structure of 802.1Q Frame. The 802.1Q header includes a 3-bit prioritization field, which allows packets to be grouped to be grouped into eight levels of priority (0-7), where level 7 is the highest one. In addition, DSL maps these eight levels to priority queues, where queue 1 has the highest priority.

For example: mark the frame of 802.1p that queued to Queue 9 on value 2.



After proper modifications, click **Save/Apply** to show the following interface.



Click **Save/Apply**. This configuration takes effective at once.

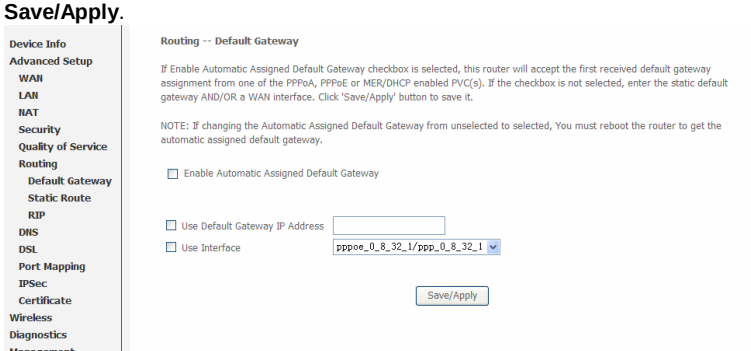
3.4.6 Routing

Click **Routing** and the **Routing** page appears. It contains the following two items: **Default Gateway** and **Static Route**.

3.4.6.1 Routing - Default Gateway

Choose **Routing** > **Default Gateway** and the following page appears. In this page, you can modify the default gateway settings.

If you select **Enable Automatic Assigned Default Gateway**, this router can accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the check box is not selected, you need to enter the static default gateway and/or a WAN interface. Then, click **Save/Apply**.



Note:

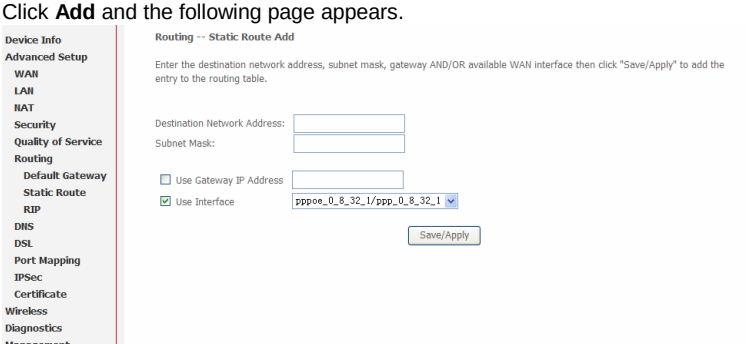
If the Automatic Assigned Default Gateway check box is changed from deselected to selected, you need to reboot the router to obtain the automatic assigned default gateway.

3.4.6.2 Routing - Static Route

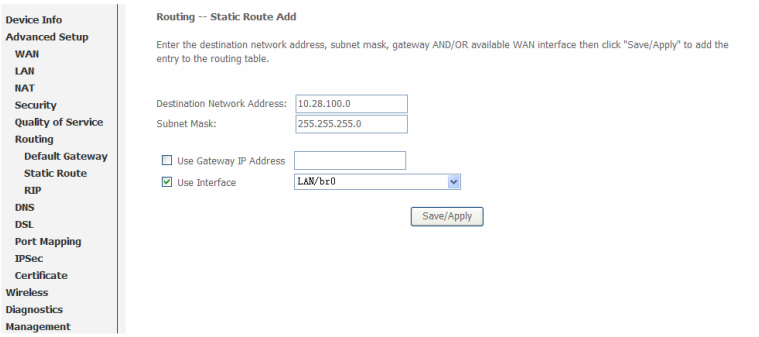
Choose **Routing** > **Static Route** and the followng page appears. In this page, you can query the preset static routes, delete an existing static route, or add a new static route. By default, the system has no static route information.

- **Destination**: The IP address to which packets are transmitted.
- **Subnet Mask**: The subnet mask of the destination IP address.
- **Gateway**: The gateway that the packets pass by during transmission.
- **Interface**: The interface that the packets pass through on the Router.

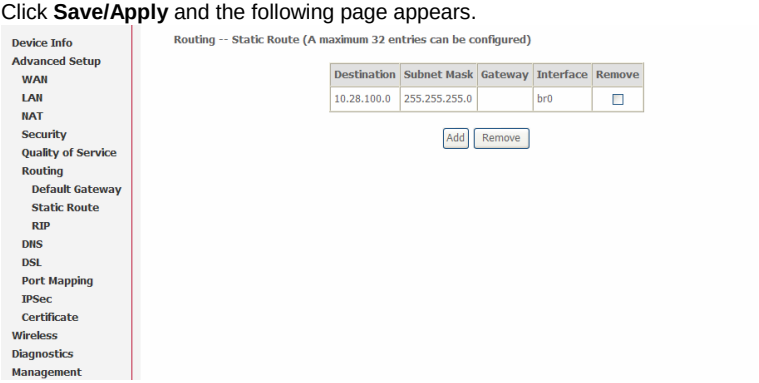
Click **Add** and the following page appears.



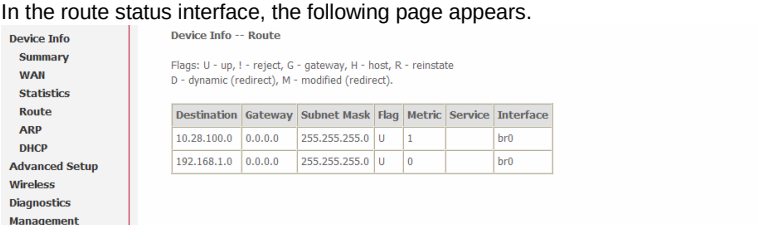
To add a static route rule, the configuration is as follows.



Click **Save/Apply** and the following page appears.



In the route status interface, the following page appears.

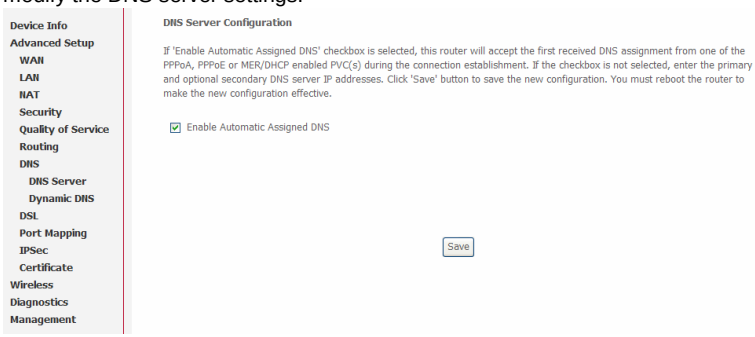


3.4.7 DNS

Click **DNS** and the **DNS** page appears. It contains the following two items: **DNS Server** and **Dynamic DNS**.

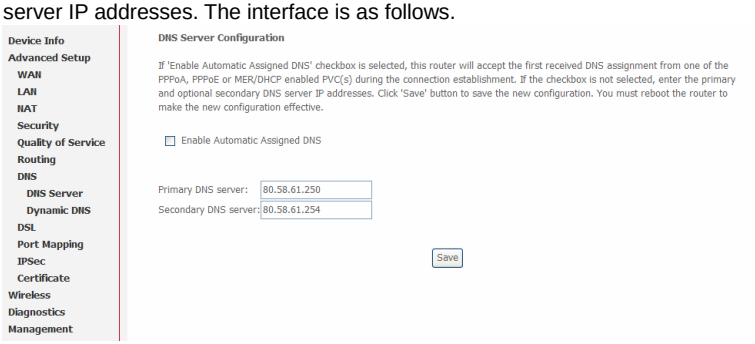
3.4.7.1 DNS Server

Choose **DNS** > **DNS Server** and the following page appears. In this page, you can modify the DNS server settings.



If select **Enable Automatic Assigned DNS**, this router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. The interface is as follows.



Click **Save** to save the new configuration.

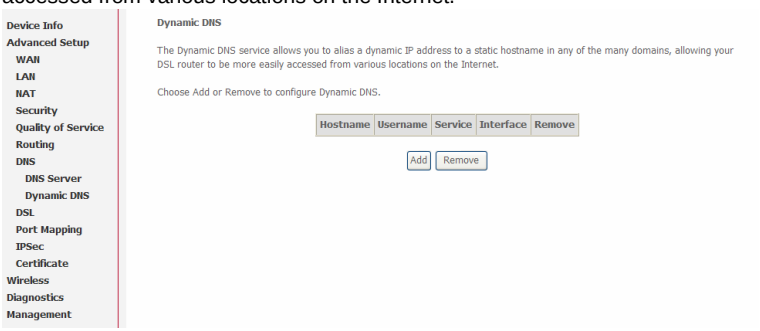
Note:

You must reboot the Router to take the new settings effect.

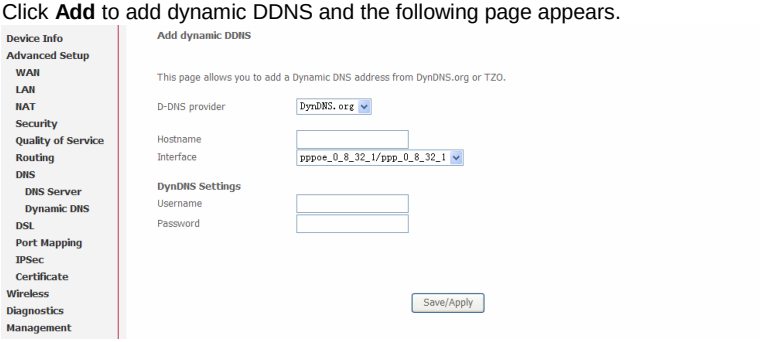
3.4.7.2 Dynamic DNS

Choose **DNS** > **Dynamic DNS** and the following page appears. In this page, you can modify the Dynamic DNS settings.

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Router to be more easily accessed from various locations on the Internet.



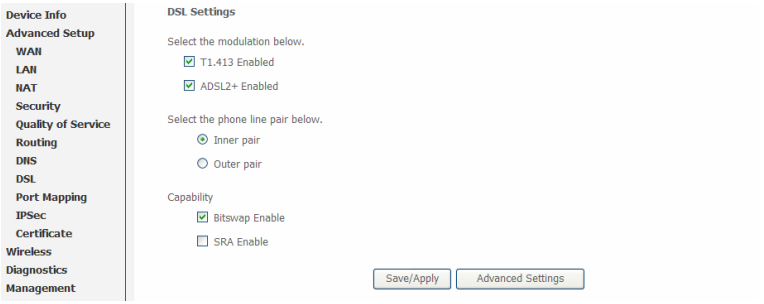
Click **Add** to add dynamic DDNS and the following page appears.



3.4.8 DSL

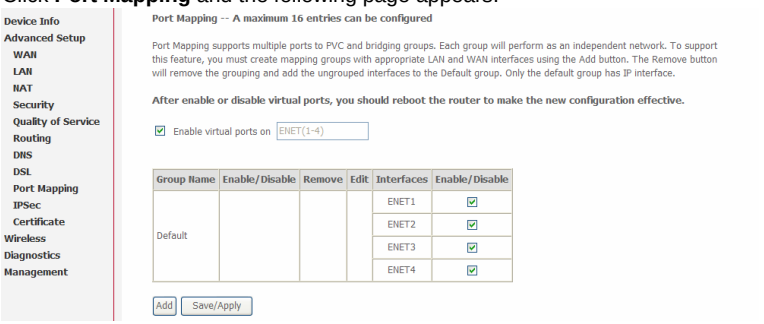
Choose **Advanced Setup** > **DSL** and the following page appears. In this page, you can modify the DSL settings.

Select one you need. But the default setting can check T1.413/ADSL2+/Inner pair/Outer pair/Bitswap/SRA. The Router can negotiate the modulation mode with the DSLAM.

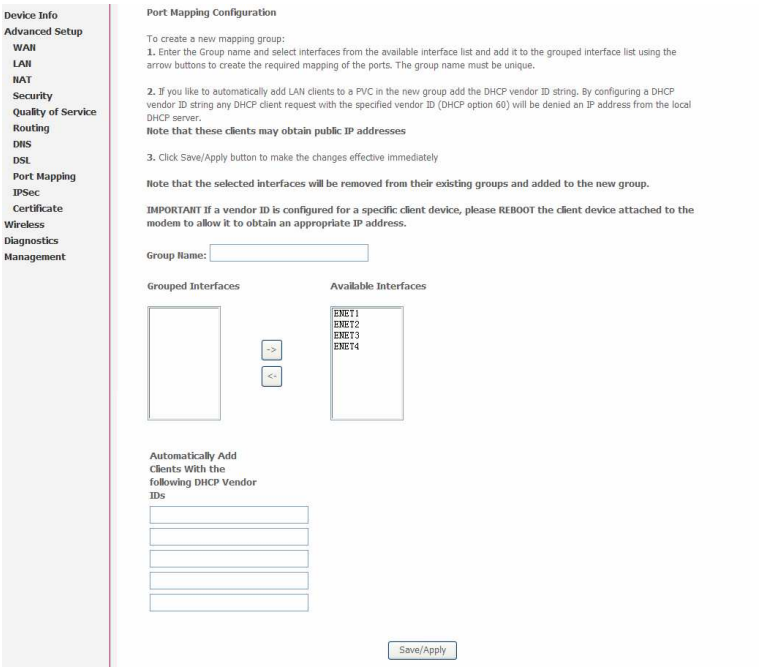


3.4.9 Port Mapping

Click **Port Mapping** and the following page appears.

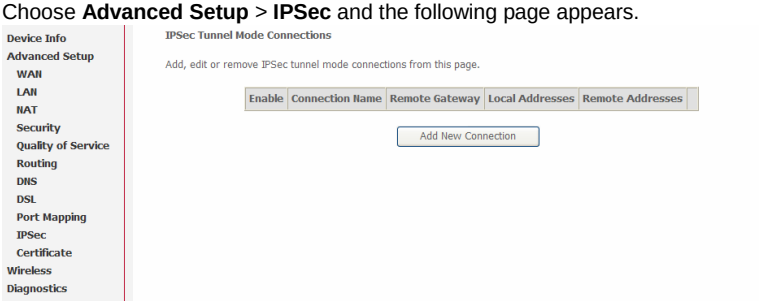


Click **Add** and the following page appears.

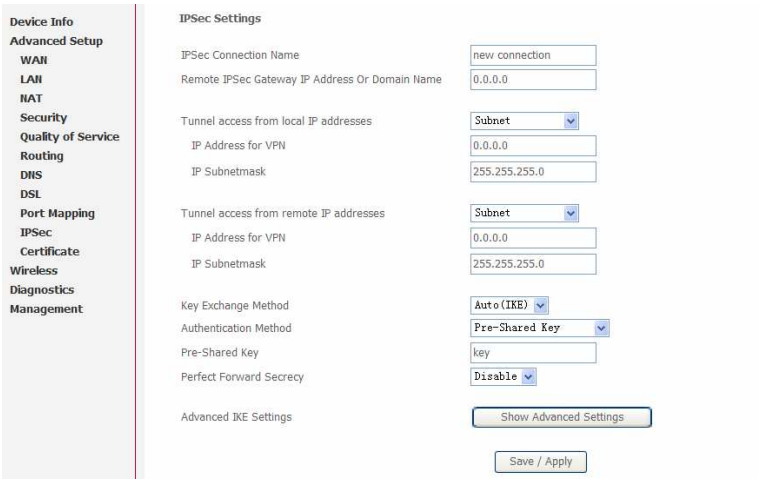


3.4.10 IPSec

Choose **Advanced Setup** > **IPSec** and the following page appears.



Click **Add New Connection** to add a new IPSec connection.



You can click **Show Advance Settings** to view some advance parameters and modify them to match the other side of this connection.

Click **Save/Apply** to save this connection, then you can check the checkbox of enable column to enable this IPSec connection. And the communication is established.

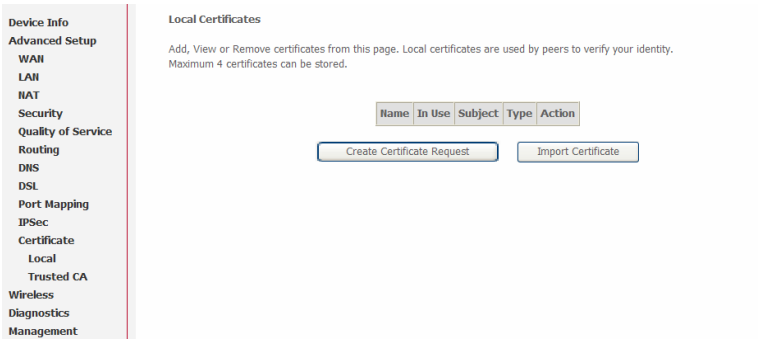
3.4.11 Certificate

Click **Certificate** and the **Certificate** page appears. It contains the following two items: **Local** and **Trusted CA**.

3.4.11.1 Local Certificates

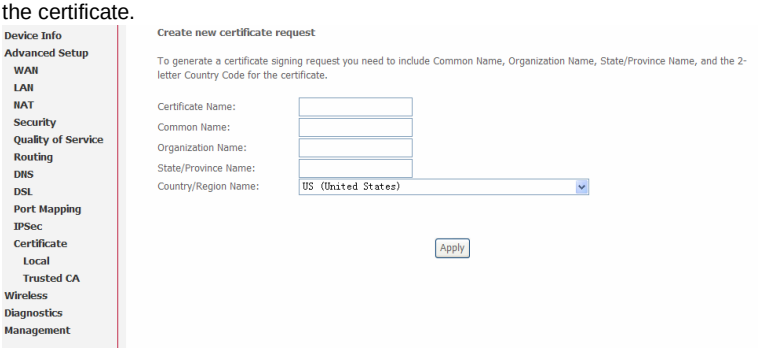
Choose **Certificate** > **Local** and the following page appears.

Local certificates are used by peers to verify your identity. It can store maximum 4 certificates.

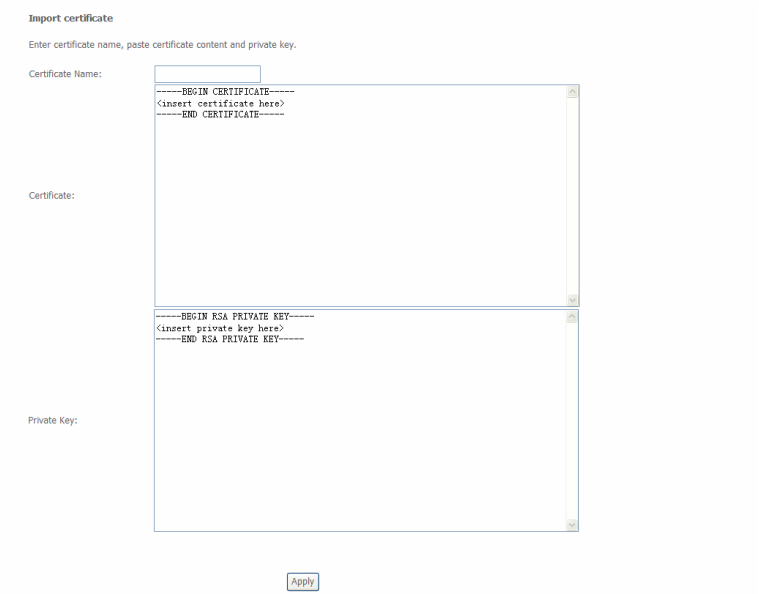


Click **Create Certificate Request** and the following page appears.

To generate a certificate signing request, you need to include **Common Name**, **Organization Name**, **State/Province Name**, and the 2-letter **Country Code** for the certificate.

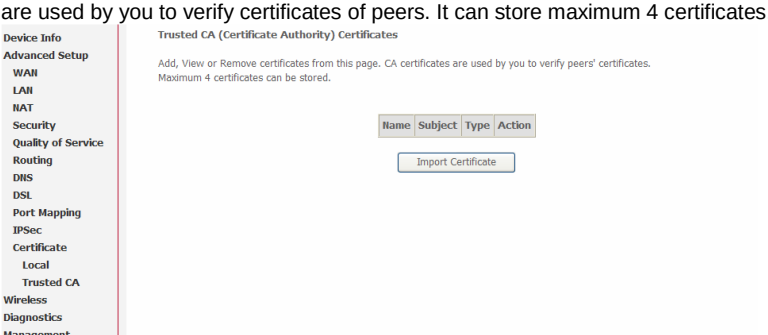


If click **Import Certificate**, the following page appears. Then you can enter certificate name, paste certificate content and private key.

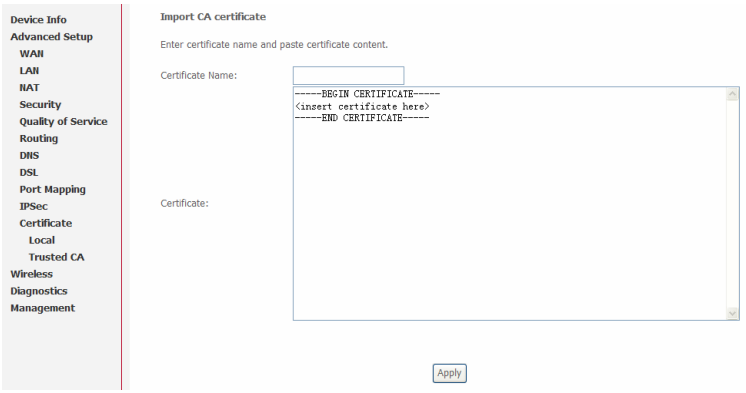


3.4.11.2 Trusted CA Certificates

Choose **Certificate** > **Trusted CA** and the following page appears. CA certificates are used by you to verify certificates of peers. It can store maximum 4 certificates.



Click **Import Certificate** and the following page appears. Then you can enter certificate name, paste certificate content.



3.5 Wireless

Click **Wireless** and you can view the following information:

- Basic
- Security
- MAC Filter
- Wireless Bridge
- Advanced
- Station Info

This section introduces the wireless LAN and some basic configurations. Wireless LAN can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points (AP) that bridge network traffic to the wired LAN.

The Router Wi-Fi® certified IEEE 802.11g compliant wireless access point allows multiple computers to connect wirelessly to your local network over the Router Wireless LAN environment. The Router is backward compatible with IEEE 802.11b, which means 802.11b and 802.11g devices can coexist in the same wireless network. The Wireless Distribution System (WDS) on your Router allows you to extend the range of your wireless network. To be able to use WDS, you will need to introduce an additional WDS-enabled access point into your wireless network. To be able to connect the computers, make sure that a wireless client adapter (WLAN client) is installed on each computer you want to connect via the WLAN.

3.5.1 Wireless LAN Basics

Some basic understanding of 802.11b/g wireless technology and terminology is useful when you are setting up the Router or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

3.5.1.1 Wireless client requirements

All wireless client adapters compliant to 802.11g and/or 802.11b can communicate with the Router (W) LAN environment. However, be aware that only 802.11g compliant wireless clients are able to gain full profit of the 54 Mb/s (Max) bandwidth delivered by the Router. It is highly recommended to use only wireless client adapters that are Wi-Fi™ certified to ensure smooth interoperability with the Router's WLAN.

3.5.1.2 Radio Transmission

Wireless LAN or WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the WLAN nodes in its broadcast range. WLAN nodes transmit digital data using FM (frequency modulation) radio signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. Digital data is superimposed onto the carrier signal. This radio signal carries data to WLAN devices within range of the transmitting device. The antennae of WLAN devices listen for and receive the signal. The signal is demodulated and the transmitted data extracted. The transmission method used by the access point is called Direct Sequence Spread Spectrum (DSSS) and operates in a range of the radio spectrum between 2.4GHz and 2.5GHz for transmission. See the expert technical specifications for more details on wireless operation.

3.5.1.3 Antennas

Direct the external antenna to allow optimization of the wireless link. If for example the antenna is erect, wireless links in the horizontal plane are favored. Please note that the antenna characteristics are influenced by the environment, that is, by reflections of the radio signal against walls or ceilings. It is advisable to use the received signal strength as indicated by the wireless client manager to optimize the antenna position for the link to a given client. Concrete walls weaken the radio signal and thus affect the connection.

3.5.1.4 Range

Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the Router in a location between the WLAN devices that maintains a roughly equal straight-line distance to all devices that need to access the Router through the wireless interface. Adding more 802.11g access points to rooms where the signal is weak can improve signal strength. Read the section about placement of the Router titled Location in the next chapter, Hardware Installation, for more information.

3.5.1.5 SSID

Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network. The Router operates in Infrastructure mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. By default the Router broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate. You may disable SSID broadcasting the wireless menu of web management.

3.5.1.6 Radio channels

The 802.11g standard allows several WLAN networks using different radio channels to be co-located. The Router supports multiple radio channels and is able to select the best radio channel at each startup. You can choose to set the channels automatically or manually.

The different channels overlap. To avoid interference with another access point, make sure that the separation (in terms of frequency) is as high as possible. It is recommended to keep at least 3 channels between 2 different access points.

The Router supports all channels allowed for wireless networking. However, depending on local regulations, the number of channels actually allowed to be used may be additionally restricted, as shown in the table below.

Regulatory Domain	Allowed Radio Channels
China	1 to 13
Europe	1 to 13
Israel	5 to 8
Japan	1 to 14
Jordan	10 to 13
Thailand	1 to 14
USA / Canada	1 to 11

3.5.1.7 Wireless Security

Various security options are available on the Router including open or WEP, 802.1x, WPA, WPA-PSK, WPA2 and WPA2-PSK. Authentication may use an open system or a shared key. For details on these methods and how to use them, please read the wireless LAN configuration information in Section 3.5.3 (Wireless Security Configuration).

3.5.1.8 About 802.11g Wireless

802.11b is an IEEE standard, operating at 2,4 GHz at a speed of up to 11 Mb/s. 802.11g, a newer IEEE standard also operating at 2,4 GHz, gives you up to 54 Mb/s speed, more security and better performance.

Today's 11-megabits-per-second 802.11b wireless networks are fine for broadband Internet access (which typically tops out at about 1 mbps) but rather slow for large internal file transfers or streaming video. However, 54-mbps, corporate-oriented 802.11a is expensive and because its radio uses the 5-GHz band and 802.11b uses the 2.4 GHz band, upgrading to an 802.11a network means either scrapping 802.11b gear or buying even-pricier hardware that can support both standards.

But 802.11g promises the same speed as 802.11a and the ability to coexist with 802.11b equipment on one network, since it too uses the 2.4-GHz band. 802.11g is an extension to 802.11b, the basis of many wireless LANs in existence today. 802.11g will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. Because of backward compatibility, an 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. You should be able to upgrade the newer 802.11b access points to be 802.11g compliant via relatively easy firmware upgrades.

Similar to 802.11b, 802.11g operates in the 2.4GHz band, and the transmitted signal uses approximately 30MHz, which is one third of the band. This limits the number of non-overlapping 802.11g access points to three, which is the same as 802.11b.

***Note**: Maximum wireless signal rate based on IEEE Standard 802.11g specifications is 54 Mbps. But actual data throughput varies depending on.network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead will cause lower actual data throughput rate.*

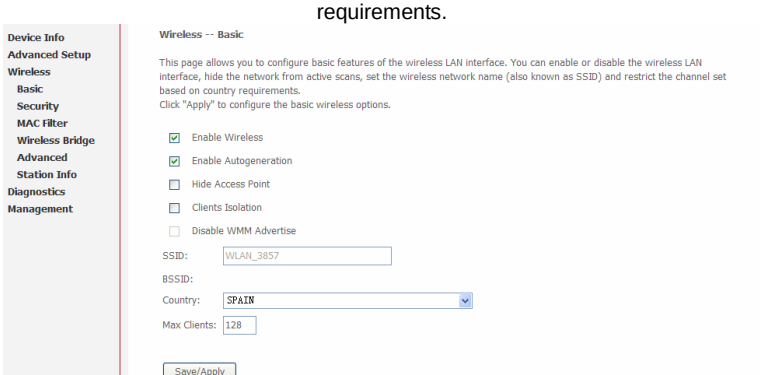
3.5.1.9 Access Point and Wireless Fidel

The Wi-Fi certification ensures that your Router will interoperate with any Wi-Fi certified 802.11g and 802.11b compliant wireless device.

The Router Wireless LAN Access Point (AP) behaves as a networking hub allowing to wirelessly interconnect several devices to the local (W) LAN and to provide access to the Internet.

3.5.2 Wireless – Basic

Choose **Wireless** > **Basic** and the following page appears. This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



- **Enable Wireless**: Select this checkbox to enable wireless function. If you disable wireless function, you can not set the parameters of this page.

- **Enable Autogeneration**: Select this checkbox to enable autogeneration function.
- **Hide Access Point**: Select this checkbox to hide any access point for your Router. Then, a station cannot obtain the SSID through passive scanning.
- **SSID**: The service set identification (SSID) is the unique name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network.
- **Country**: Select the country where you are located. The channel adjusts according to the country.

After setting, click **Save/Apply** to apply the settings.

3.5.3 Wireless – Security

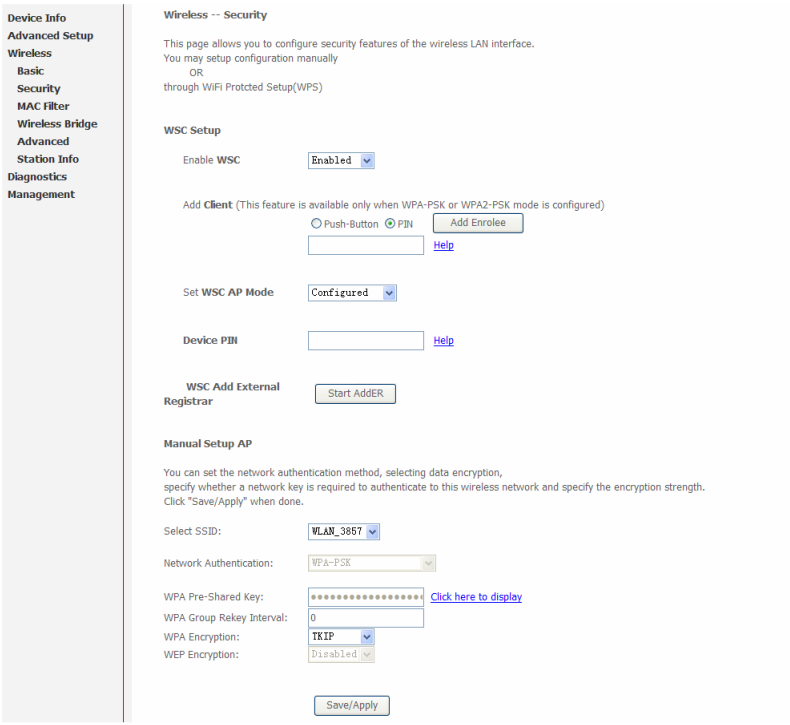
Choose **Wireless** > **Security** and the following page appears. This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

This device is equipped with 802.1X and WPA/WPA2 (Wi-Fi Protected Access), the latest security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). By default, wireless security is disabled and authentication is open. Before enabling the security, consider your network size, complexity, and existing authentication infrastructure and then determine which solution applies to it.

Following is a description of the different options.

- Select SSID: Select the wireless LAN of SSID to configure security features.
- No Encryption: Please refer to below for details of configuration
- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open.
- WEP Encryption: Disable WEP Encryption.

The data is not encrypted when it is transferred from the device to the client station. This is the default option.



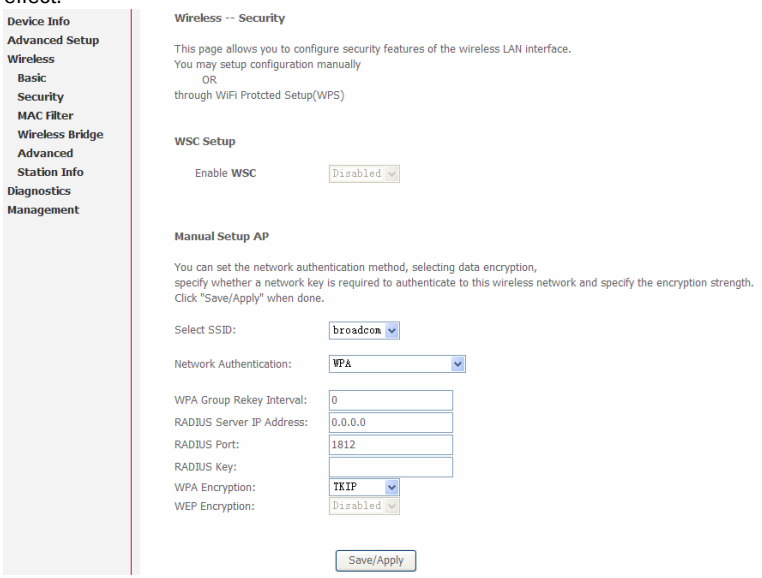
Click **Save/Apply** to save the wireless security options and make the modification effect.

WPA Authentication

- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA.
- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- Radius Server IP Adress: Enter the IP Address of the authentication server.
- Radius Port: Enter the port number of the authentication server. The default port number is 1812.
- Radius Key: Enter the same key as the Radius server's.

- WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.

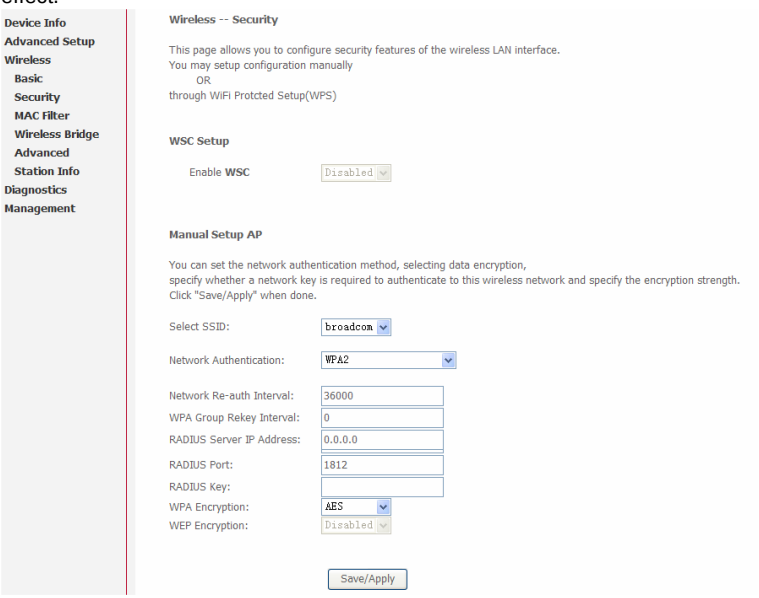


WPA2 Authentication

- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA2.
- WPA2 Preauthentication: Selec Enable or Disenable.
- Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- RADIUS Server IP Adress: Enter the IP Address of the authentication server.
- RADIUS Port: Enter the port number of the authentication server. The default port number is 1812.

- RADIUS Key: Enter the same key as the Radius server's.
- WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



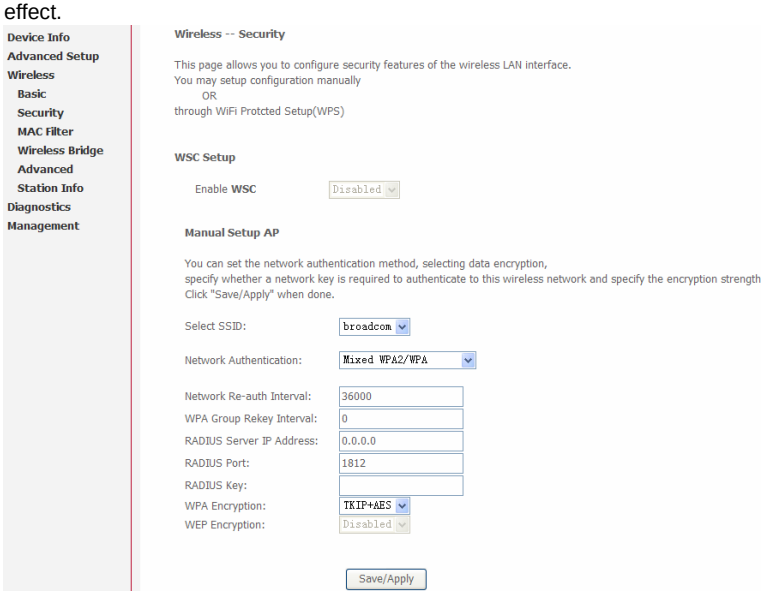
Mixed WPA2/WPA Authentication

This authentication mode means AP auto adjust to use WPA2 or WPA according to wireless clients.

- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA.
- WPA2 Preauthentication: Selec Enable or Disenable.
- Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.

- Radius Server IP Adress: Enter the IP Address of the authentication server.
- Radius Port: Enter the port number of the authentication server. The default port number is 1812.
- Radius Key: Enter the same key as the Radius server's.
- WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



WPA-PSK Authentication

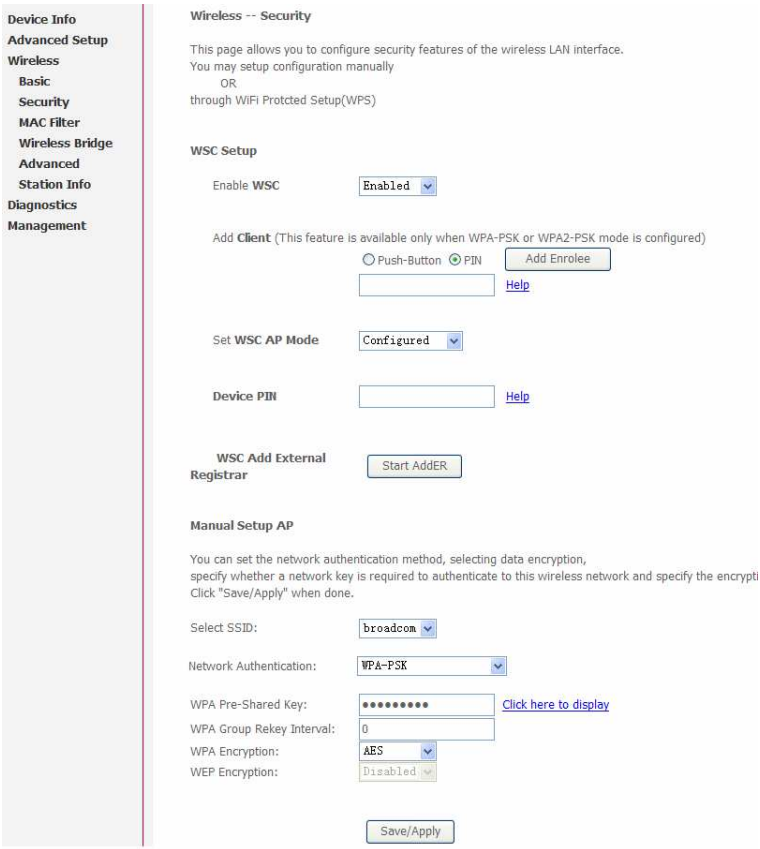
- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA-PSK.
- WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters

ASCII	8	63
Hexadecimal	8	64

- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



WPA2-PSK Authentication

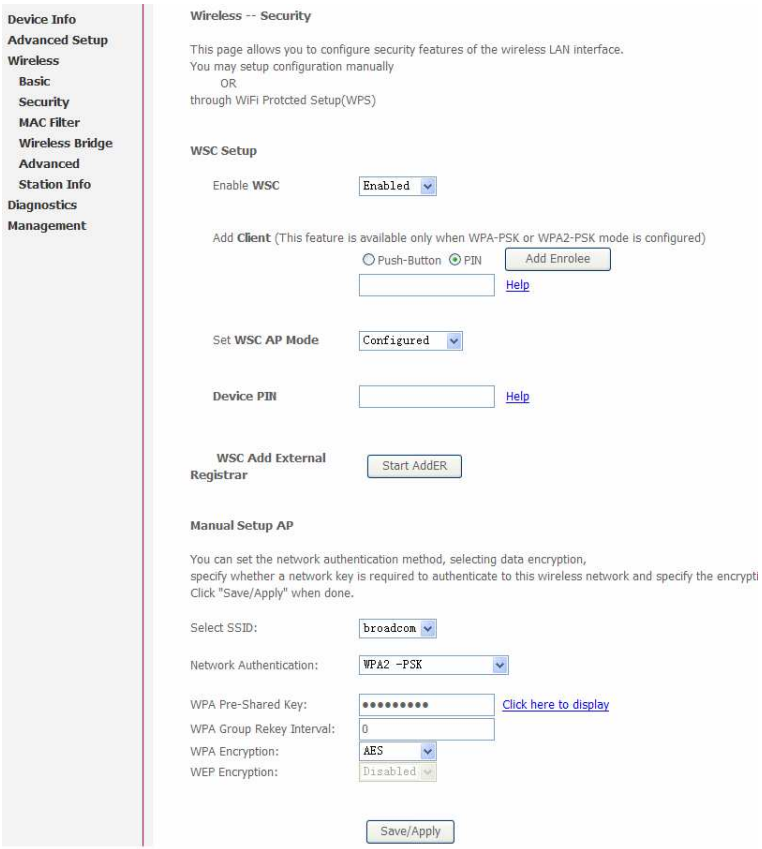
- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2-PSK.
- WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63

Format	Minimum characters	Maximum Characters
Hexadecimal	8	64

- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



Mixed WPA2/WPA-PSK Authentication

This authentication mode means AP auto adjust to use WPA2-PSK or WPA-PSK according to wireless clients.

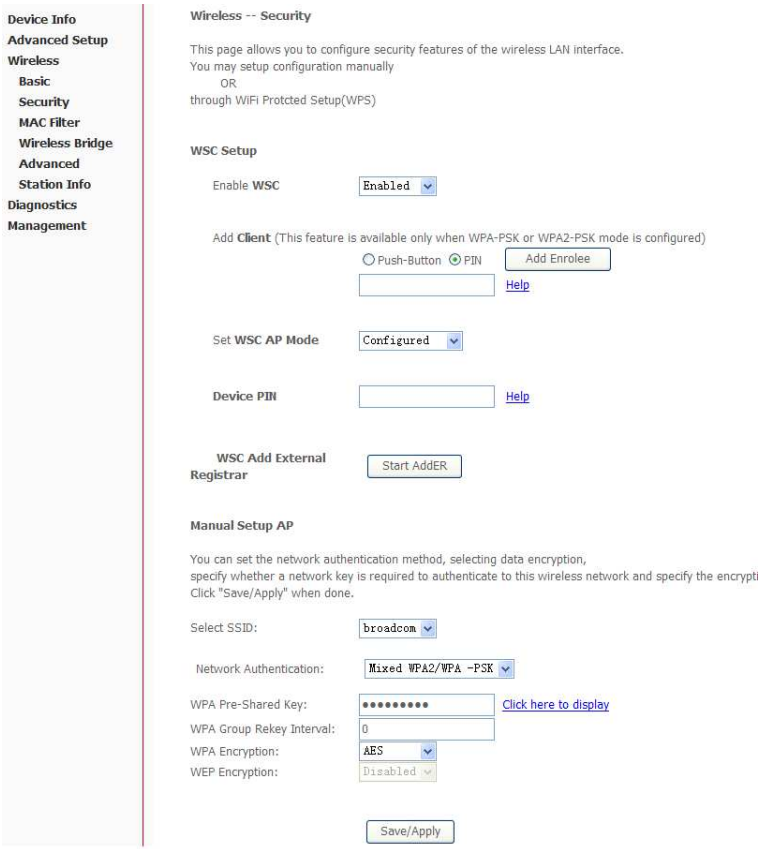
- Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA-PSK.
- WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum	Maximum

	characters	Characters
ASCII	8	63
Hexadecimal	8	64

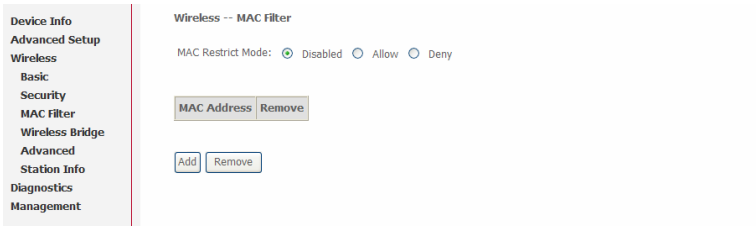
- WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.



3.5.4 Wireless - MAC Filter

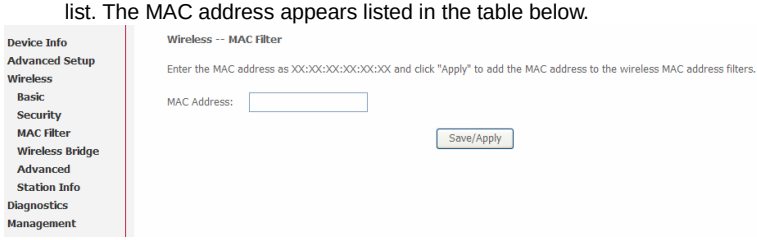
Choose **Wireless** > **MAC Filter** and the following page appears. This page allows you to create a list of MAC addresses that are banned or allowed association with the wireless access point.



- **MAC Restrict Mode:** You can select **Disabled**, **Allow**, or **Deny**.
  - Select **Disabled** to disable MAC filter function.
  - Select **Allow**, the wireless MAC address in the wireless access control list is permitted to access the Router.
  - Select **Deny**, the wireless MAC address in the wireless access control list is denied to access the Router.
- **Remove a MAC Access Control:** After selecting the MAC address in the table, and click **Remove** to remove the MAC address.

Set the MAC filter to **Allow** or **Deny**, then click **Add** to add a wireless MAC address to you wireless access control list. The following page appears.

- **Add a MAC Access Control:** To add a new MAC address to your wireless MAC address filters, click **Add** to show next page. Type in the MAC Address in the entry field provided. Click **Save/Apply** to add the MAC address to the list. The MAC address appears listed in the table below.



MAC Address: Enter the MAC address that is permitted or allowed for accessing the Router.

After setting, click **Save/Apply** to apply the settings.

3.5.5 Wireless – Bridge

Choose **Wireless** > **Bridge** and the following page appears. This page allows you to configure wireless bridge features of the wireless LAN interface.

The Wireless Distribution System (WDS) allows you to extend the range of your wireless network by introducing one or more WDS-enabled devices into your wireless network. You can only establish WDS links with WDS-enabled devices.

You can manually enter Remote Bridges MAC Address to the list. You can also do it automatically in the following steps:

Step 1 In the Bridge Restrict list, click Enabled (Scan).

Step 2 Click Refresh to update the remote bridges.

The router waits for a few seconds to update. And then lists the results in the Accessible Access Points table.

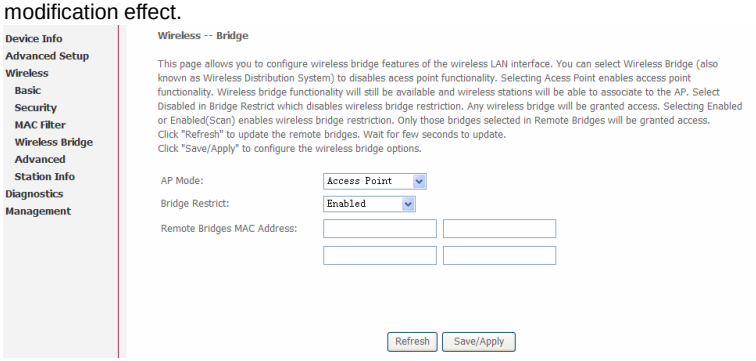
Step 3 Check on the box in the left column of the list for selecting the Access Point to which you want to establish a WDS connection.

Step 4 Click **Save/Apply**.

You must configure all Bridges Access Point with:

- The same encryption and authentication mode as Open, Shared, WEP, WPA-PSK or WPA2-PSK.
- The same fixed channel.

Click **Save/Apply** to configure the wireless bridge options and make the modification effect.

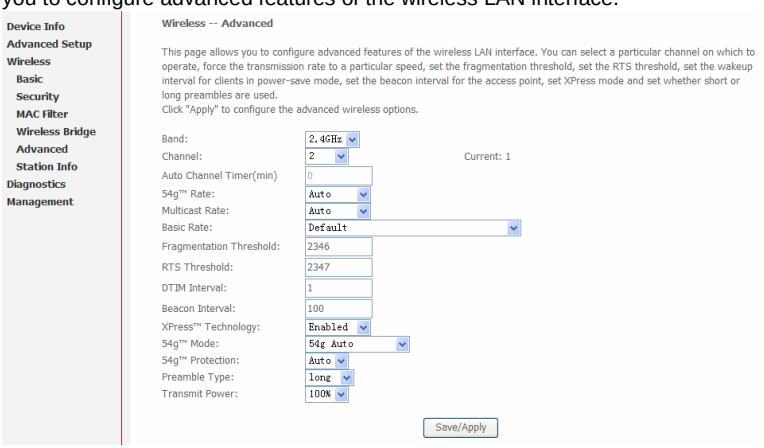


- **AP Mode:** You can select **Access Point** or **Wireless Bridge** from the drop-down list.
  - Select **Wireless Bridge** (also known as WDS) to disables access point functionality.
  - Select **Access Point** to enable access point functionality. The Wireless bridge functionality is also available and wireless stations are able to associate to the AP.

- **Bridge Restrict:** You can select **Enabled**, **Enabled (Scan)**, or **Disabled** from the drop-down list.
- Select **Disabled** to disable bridge restriction function. Any wireless bridges are allowed to access.
- Select **Enabled** or **Enabled (Scan)** to enable bridge restriction function. Only the bridges whose MAC addresses are listed in the **Remote Bridge MAC Address** field are allowed to access.

3.5.6 Wireless – Advanced

Choose **Wireless** > **Advanced** and the following page appears. This page allows you to configure advanced features of the wireless LAN interface.



- **Band:** Select the wireless frequency band. The router operates in the 2.4GHz.
- **Channel:** Select the appropriate channel to correspond with your network settings. You can select **Auto or 1~13** from the drop-down list. All devices in your wireless network must operate in the same channel in order to work correctly.
- **Auto Channel Timer (min):** Specifies the time of auto channeling.
- **54g™ Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and

enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

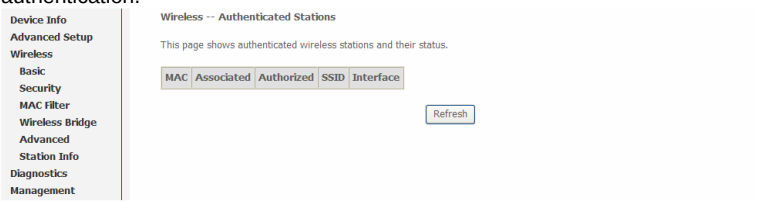
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** Beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **XPress™ Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.

- **54g™ Mode:** Compatible with IEEE 802.11b, IEEE 802.11g. Select a Standards from the drop-down list box. Its default setting is 54g Auto. The drop-down list box includes below mode.
- **802.11b Only**: Only stations that are configured in 802.11b mode can associate. If you select it, the rate of transmission only has selected values: 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps. For other selections, the rate of transmission has lots of selected values: 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 9Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps.
- **54g LRS**: This is a special compatibility mode for 802.11b/g and is in fact designed for older types of b-clients. Use this mode if you are experiencing problems with wireless clients that connect to the Access Point. If you select it, the preamble type will be disabled, which cannot be set.
- **54g Auto**: Only stations that are configured in 802.11b/g mode can associate.
- **54g Perfomance**: Only stations that are configured in 802.11g mode can associate. It is the same as 54g LRS, if you select it, the preamble type will be disabled, which cannot be set.
- **54g™ Protection**: The 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
- **Preamble Type**: Preambles are a sequence of binary bits that help the receivers synchronize and ready for receipt of a data transmission. Some older wireless systems like 802.11b implementation use shorter preambles. If you are having difficulty connecting to an older 802.11b device, try using a short preamble. You can select short preamble only if the 54g mode is set to 802.11b.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.

Click **Save/Apply** to save the settings.

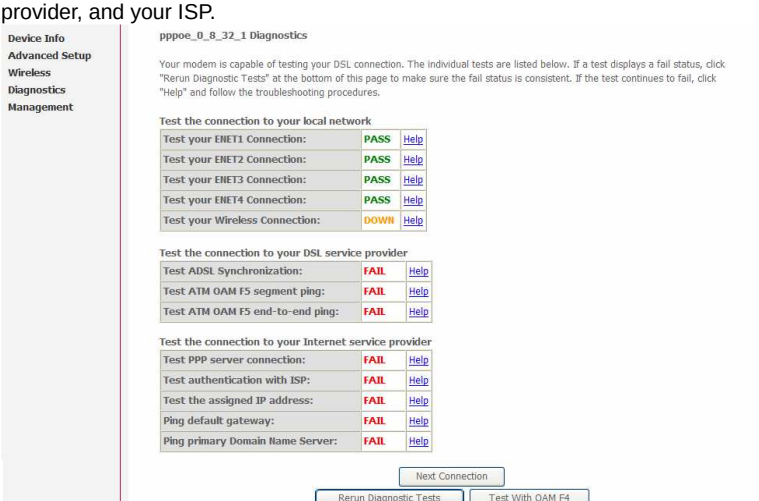
3.5.7 Wireless – Station Info

Choose **Wireless** > **Station Info** and the following page appears. This page shows authenticated wireless stations and their status about association and authentication.



3.6 Diagnostics

Click **Diagnostics** and the following page appears. In this page, you can test the DSL connection of the Router. It displays the connection to LAN, DSL service provider, and your ISP.



If the connection is failed, click **Rerun Diagnostic Tests** to check the connection status.

3.7 Management

Click **Management** and you can view the following information:

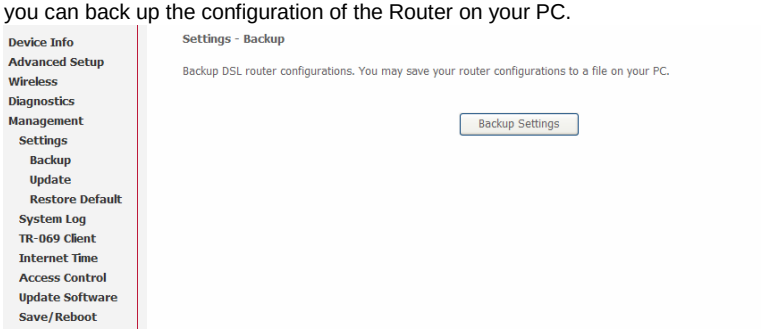
- Settings
- System Log
- TR-069 Client
- Internet Time
- Access Control
- Update Software
- Save/Reboot

3.7.1 Settings

Click **Settings** and the **Settings** page appears. It contains the following three items: **Backup**, **Update**, and **Restore Default**.

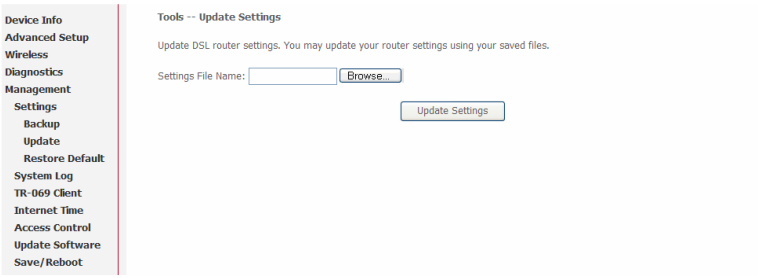
3.7.1.1 Backup

Choose **Settings** > **Backup Settings** and the following page appears. In this page, you can back up the configuration of the Router on your PC.



3.7.1.2 Update

Choose **Settings** > **Update** and the following page appears. In this page, you can upgrade the software of the Router and select the correct update configure settings file. Then, click **Update Settings** to update the Router settings.



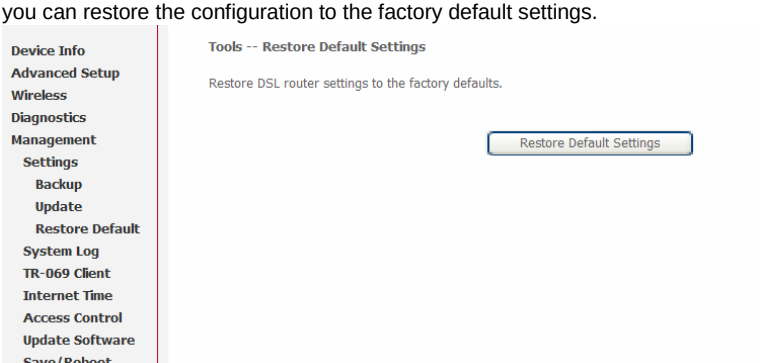
The procedure of upgrading the software is as follows:

Step 1 Click **Browse** to select the upgrading configuration file.

Step 2 Click **Update Settings** to upgrade the configuration file.

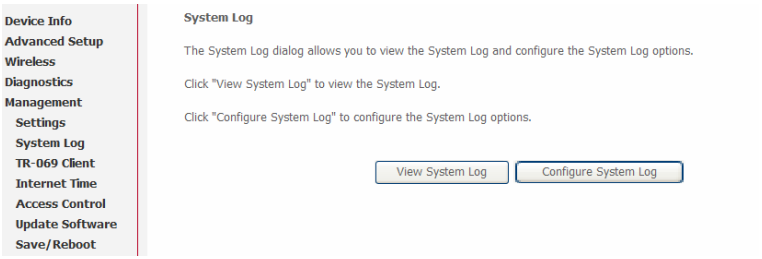
3.7.1.3 Restore Default

Choose **Settings** > **Restore Default** and the following page appears. In this page, you can restore the configuration to the factory default settings.

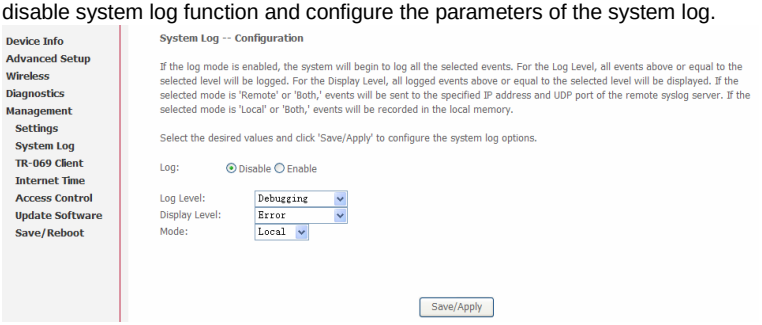


3.7.2 System Log

Choose **Management** > **System Log** and the following page appears.



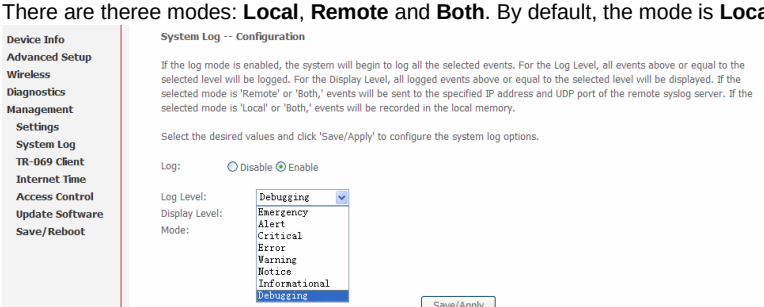
Click **Configure System Log** and the following page appears. You can enable or disable system log function and configure the parameters of the system log.



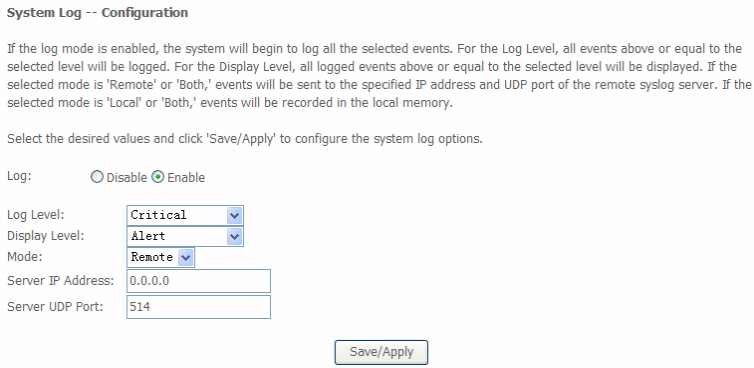
Select **Enbale** to enable system log function.

There are eight levels in the **Log Level** filed and **Display Level** field: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Informational**, and **Debugging**. By defaut, the log level is **Debugging**, the display level is **Error**.

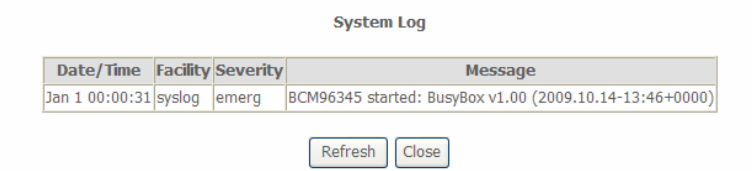
There are theree modes: **Local**, **Remote** and **Both**. By default, the mode is **Local**.



If you set the mode to **Remote** or **Both**, all events are transmitted to the specified UDP port of the specified log server.



After setting, click **Save/Apply** to take the settings effect. Then click **View System Log** to view the system logs.



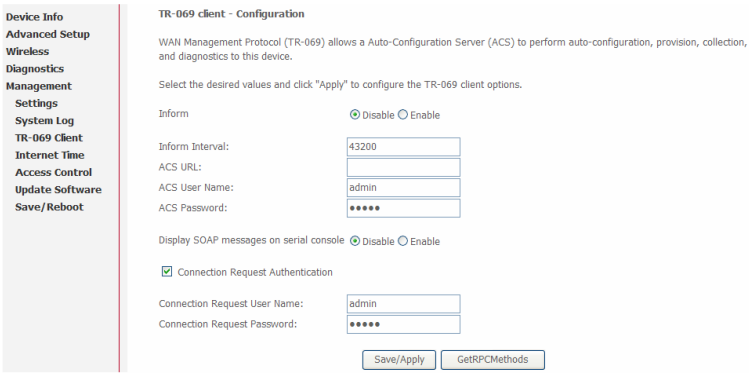
Click **Refresh** to refresh the system event logs or click **Close** to logout this page.

Note:

The system logs the events that are superior or equal to the specified level. If you want to record all the logs, you need to set the level to **Debugging**.

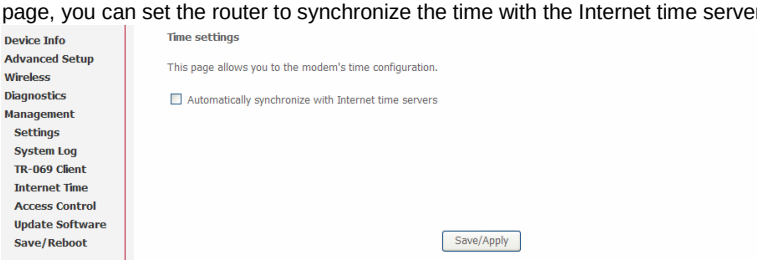
3.7.3 TR-069 Client

Choose **Management** > **TR-069 Client** and the following page appears. In this page, you can configure TR-069 parameters of the router.

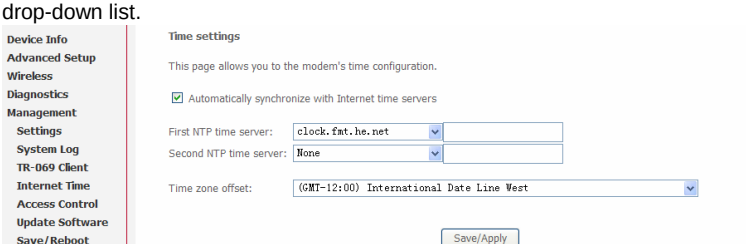


3.7.4 Internet Time

Choose **Management** > **Internet Time** and the following page appears. In this page, you can set the router to synchronize the time with the Internet time server.



Select the checkbox of **Automatically synchronize with Internet time servers**, and the following page appears. In this page, you can select the specified Network Time Protocol (NTP) time server and time zone in which you are located from the drop-down list.

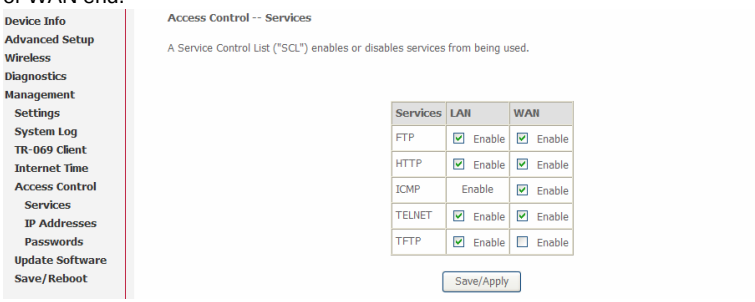


3.7.5 Access Control

Click **Access Control** and the **Access Control** page appears. It contains the following three items: **Services**, **IP Address**, and **Passwords**.

3.7.5.1 Services

Choose **Access Control** > **Services** and the following page appears. In this page, you can enable or disable FTP, HTTP, ICMP, Telnet, and TFTP services at the LAN or WAN end.

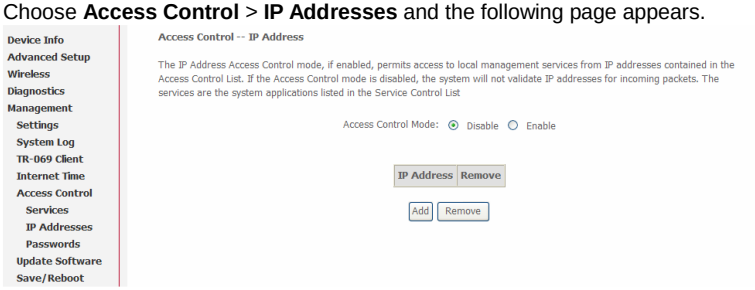


Note:

If the connection is PPPoE PVC, you can view the information of WAN side.

3.7.5.2 IP Addresses

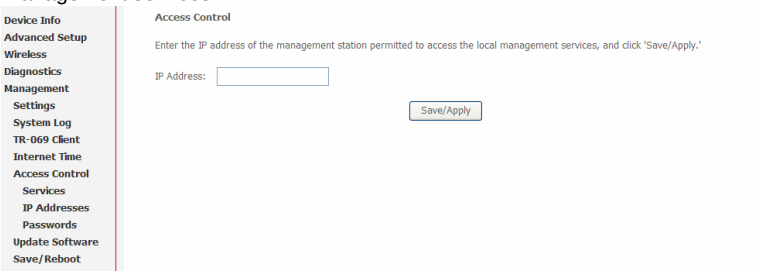
Choose **Access Control** > **IP Addresses** and the following page appears.



Set the access control mode to **Enable**, then the router permits the IP address in the access control list (ACL) to access the local management services.

If set the access control mode to **Disable**, then the router does not permit IP addresses to access the services. The services are listed in the service control list of the **Services** page.

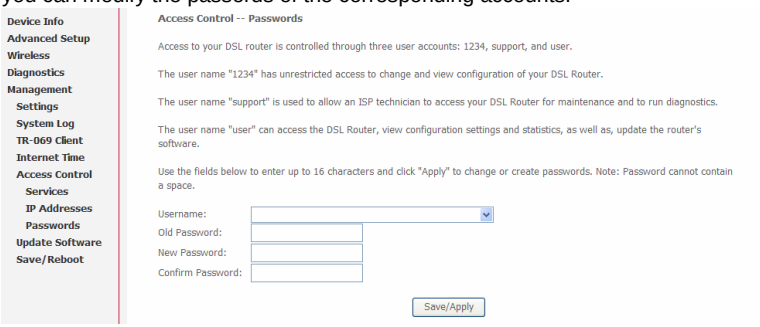
Click **Add** to add an IP address and the following page appears. Enter the IP address of the management station that is permitted to access the local management services.



After setting, click **Save/Apply** to apply the settings.

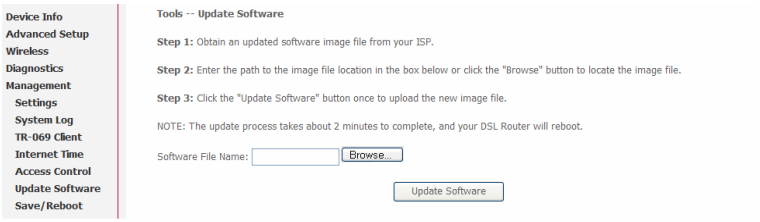
3.7.5.3 Passwords

Choose **Management** > **Passwords** and the following page appeas. In this page, you can modify the passords of the corresponding accounts.



3.7.6 Update Software

Choose **Management** > **Update Firmware** and the following page appears. In this page, you can update the software of the Router.



Click **Browse** to select the software file. Then click **Update Firmware** to start updating the software.

Caution:

Do not turn off the Router or press the Reset button while the procedure is in progress. After updating the software, the Router reboots automatically. You need to guarantee the updating software is accurate.

After updating the software, it is recommended to reset the configuration to the factory default configuration.

3.7.7 Save/Reboot

Choose **Management** > **Save/Reboot** and the following page appers. In this page, you can reboot the Router.

Click Save/Reboot to reboot the Router.